TRANSACTIONS

OF THE

AMERICAN MATHEMATICAL SOCIETY

EDITED BY

MAXIME BÔCHER

HENRY SEELY WHITE LEONARD EUGENE DICKSON

WITH THE COÖPERATION OF

GILBERT A. BLISS JOHN I. HUTCHINSON EDWARD KASNER

MAX MASON FOREST R. MOULTON PERCEY F. SMITH

ERNST J. WILCZYNSKI EDWIN B. WILSON

VOLUME 12,
1911

PUBLISHED BY THE SOCIETY
LANCASTER, PA., AND NEW YORK
1911

510.6
AMS
N.12

PRESS OF
THE NEW ERA PRINTING COMPANY
LANCASTER, PA

TABLE OF CONTENTS

VOLUME 12 1911

PAGES

BATES, WILLIAM HUNT, of LaFayette, Ind. An application of symbolic methods to the treatment of mean curvatures in hyperspace . . . 19

BIRKHOFF, GEORGE D., of Princeton, N. J. General theory of linear difference equations 243

BLICHFELDT, H. F., of Stanford University, Cal. On the order of linear homogeneous groups (Fourth paper). 39

CARMICHAEL, R. D., of Princeton, N. J. Linear difference equations and their analytic solutions 99

COBLE, ARTHUR B., of Baltimore, Md. An application of Moore's cross-ratio group to the solution of the sextic equation. 311

COOLIDGE, JULIAN LOWELL, of Cambridge, Mass. The metrical aspect of the line-sphere transformation. 43

DICKSON, LEONARD EUGENE, of Chicago, Ill. An invariantive investigation of irreducible binary modular forms 1

———— A fundamental system of invariants of the general modular linear group with a solution of the form problem. 75

EIESLAND, JOHN, of Morgantown, W. Va. On minimal lines and congruences in four-dimensional space 403

EVANS, GRIFFITH C., of Cambridge, Mass. Volterra's integral equation of the second kind, with discontinuous kernel. Second paper. . . 429

GLENN, O. E., of Philadelphia, Penn. On semi-discriminants of ternary forms 367

HEDRICK, EARLE RAYMOND, of Columbia, Mo. On properties of a domain for which any set is closed 285

KASNER, EDWARD, of New York City. Natural systems of trajectories generating families of Lamé 70

MANNING, W. A., of Stanford University, Cal. On the limit of the degree of primitive groups. 375

MILLER, G. A., of Urbana, Ill. On the use of the co-sets of a group. . 326

———— Isomorphisms of a group whose order is a power of a prime. 387

MITCHELL, HOWARD H., of New Haven, Conn. Determination of the ordinary and modular ternary linear groups 207

215592

PAGES

MOORE, CHARLES N., of Cincinnati, Ohio. On the uniform convergence of the developments in Bessel's functions 181

PELL, ANNA JOHNSON, of Chicago, Ill. Biorthogonal systems of functions. 135

———— Applications of biorthogonal systems of functions to the theory of integral equations 165

ROEVER, WILLIAM H., of St. Louis, Mo. The southerly deviation of falling bodies 335

ROWE, J. E., of Baltimore, Md. Important covariant curves and a complete system of invariants of a rational quartic curve 295

SNYDER, VIRGIL, of Ithaca, N. Y. An application of a (1, 2) quaternary correspondence to the Kummer and Weddle surfaces 354

WILCZYNSKI, E. J., of Chicago, Ill. One parameter families and nets of plane curves 473

Notes and errata: volumes 10 and 11. 511

AN INVARIANTIVE INVESTIGATION OF IRREDUCIBLE BINARY MODULAR FORMS*

BY

LEONARD EUGENE DICKSON

1. A fundamental system of invariants of the group of all binary linear transformations in a finite field is shown in §§ 2–6 to consist of two invariants, one the product of the distinct linear forms and the other the product of the distinct irreducible quadratic forms, where in each case no two factors have a constant ratio. The product π_m of the irreducible forms of degree m can be expressed in terms of the fundamental invariants; this is accomplished in §§ 7–9 by means of the remarkable three-term recursion formula (15).

Two forms shall be said to belong to the same class if and only if one of them can be transformed into a constant multiple of the other by a linear transformation of determinant unity in the field. It is shown in § 10 that there are as many classes of irreducible binary forms of degree m as there are irreducible factors of π_m when expressed as a function of a certain pair of invariants. The choice of the latter is different in the two cases $p = 2$, $p > 2$, where p is the modulus of the field; this is due to the fact that, in the respective cases, there are one or two similarity transformations of determinant unity. The investigation is completed for the values of m less than 8. The difficulties encountered increase as the number of factors of m increases. Certain problems arise for which the present invariantive theory affords an indirect solution, whereas a direct solution appears to be quite difficult (cf. end of § 10, and end of § 17). For $m = 6$, it was necessary to enumerate the irreducible cubics in the $GF[p^n]$ whose roots are squares in the $GF[p^{3n}]$ and have a given sum.

Determination of a Fundamental System of Invariants, §§ 2–6.

2. Let G be a group of finite order g composed of linear homogeneous transformations on $m\,(m > 1)$ variables with coefficients in any given field F. The term point will be used in the sense of homogeneous coördinates, so that $(x_1, \cdots, x_m)$ is identified with $(\mu x_1, \cdots, \mu x_m)$, while $(0, \cdots, 0)$ is excluded.

* Presented to the Society, September 7, 1910.

A transformation which leaves every point unaltered is necessarily a similarity transformation

$$x_i' = ax_i \qquad (i=1, \cdots, m). \tag{1}$$

In fact, by employing the points all but one of whose coördinates are zero, we see that the transformation is of the form

$$x_i' = a_i x_i \qquad (i=1, \cdots, m).$$

Then by employing the points all but two of whose coördinates are zero, we see that the a_i are equal. Let γ be the number of transformations (1) contained in G, and set $\omega = g/\gamma$. We assume that $\omega > 1$. Any point is one of at most ω distinct conjugates under G. A point is called special if it is one of fewer than ω conjugates, that is, if it is invariant under at least one transformation other than (1) of the group G. If a point P is invariant under T and if S replaces P by P', then P' is invariant under $S^{-1}TS$. To determine all special points it therefore suffices to employ a representative of each set of conjugate transformations other than (1), obtain the points invariant under the representative, select the distinct points so obtained, and find the conjugates to each under G.

3. Let G be the group of all binary linear homogeneous transformations of determinant unity in the Galois field $GF[p^n]$ of order p^n. The order of G is

$$g = p^n(p^{2n}-1). \tag{2}$$

Within G any transformation with irreducible characteristic determinant $\Delta(\rho)$ is equivalent to a transformation *

$$T = \begin{pmatrix} \alpha & -1 \\ 1 & 0 \end{pmatrix}, \qquad \Delta(\rho) = \rho^2 - \rho\alpha + 1.$$

The only points invariant under T are $(\rho, 1)$, where $\Delta(\rho) = 0$. The transformations of G which leave $(\rho, 1)$ unaltered are

$$\begin{pmatrix} b & -c \\ c & b - c\alpha \end{pmatrix}, \qquad b^2 - \alpha bc + c^2 = 1,$$

namely, the transformations commutative with T. The quadratic condition may be written in the form

$$(b - \rho c)^{p^n+1} = 1,$$

where ρ is a root of $\Delta(\rho) = 0$, and hence has $p^n + 1$ sets of solutions in the $GF[p^n]$. Thus $(\rho, 1)$ is one of $p^{2n} - p^n$ conjugate points under G. The resulting system of special points is therefore $(e\rho + f, 1)$, where e is any element

* These Transactions, vol. 2 (1901), p. 117.

$\neq 0$ of the $GF[p^n]$ and f is any element. Such a point together with $(\epsilon\bar{\rho}+f, 1)$, where $\bar{\rho}$ is the second root of $\Delta(\rho)=0$, determine a quadratic form $x^2+\cdots$ which vanishes only for these two points. Hence a relative invariant under G is given by the product Q of the $\frac{1}{2}(p^{2n}-p^n)$ irreducible quadratic forms $x^2+\cdots$. We have *

$$Q=\frac{x^{p^{2n}-1}-y^{p^{2n}-1}}{x^s-y^s}=\sum_{j=0}^{p^n} x^{s(p^n-j)}y^{sj} \qquad (s=p^n-1). \tag{3}$$

Consider next a transformation S for which

$$\Delta(\rho)=(\rho-\kappa)(\rho-\kappa^{-1}),$$

where κ is in the $GF[p^n]$. There exists a linear function l which S replaces by κl. If $\kappa^2\neq 1$, S is therefore equivalent within G with $\left(\begin{smallmatrix}\kappa & 0\\ 0 & \kappa^{-1}\end{smallmatrix}\right)$, which leaves only (1, 0) and (0, 1) unaltered. If $\kappa^2=1$, S is equivalent to

$$S_\beta=\begin{pmatrix}\pm 1 & 0\\ \beta & \pm 1\end{pmatrix}.$$

Since S_0 is of type (1), we may set $\beta\neq 0$; then S_β leaves only (0, 1) invariant. Hence when $\Delta(\rho)$ is reducible, the resulting system of special points is composed of the p^n+1 points (1, 0) and $(a, 1)$, where a ranges over the field. There results the relative invariant

$$L=y\prod_a(x-ay)=x^{p^n}y-xy^{p^n}. \tag{4}$$

4. **Lemma.** *If an integral function is invariant under the group G of all m-ary linear homogeneous transformations of determinant unity in the $GF[p^n]$, it is an absolute invariant of G.*

The group G is generated † by transformations of the type $B_{rs\lambda}$, which alters only one variable x_r, replacing it by $x_r+\lambda x_s$. If B multiplies a function by μ, B^p multiplies it by μ^p. Now B is of period p. Hence $\mu^p=1$. Employing the power p^{n-1}, we get

$$\mu^{p^n}=\mu=1.$$

5. We may now prove that any integral invariant I of the binary group G is an integral function of the invariants Q and L. If I vanishes for a special point it has the factor Q or L. It remains to investigate the invariants I which vanish for no special point. The number of transformations (1) contained in G is

$$\gamma=1 \text{ if } p=2, \qquad \gamma=2 \text{ if } p>2. \tag{5}$$

* DICKSON, *Linear Groups* (Leipzig, 1903), page 17.

† *Linear Groups*, page 78.

Any non-special point is one of $\omega = g/\gamma$ conjugates under G. Now the forms

$$q = Q^{(p^n+1)/\gamma}, \qquad l = L^{p^n(p^n-1)/\gamma} \tag{6}$$

are of degree ω. Let F_{p^n} be the field composed of all roots of all algebraic equations with coefficients in the $GF[p^n]$. The invariant I vanishes for a set of ω conjugate points; if (c, d) is one of these points, the ratio $c:d$ belongs to the field F_{p^n}. Hence we can determine τ in the latter field such that $q(c, d) + \tau l(c, d) = 0$. Thus I has the factor $q + \tau l$, and I is a product of such linear functions of q, l. If I has its coefficients in the $GF[p^n]$, and τ is a root of an equation of degree t irreducible in the $GF[p^n]$, the presence of the factor $q + \tau l$ in I implies that of the conjugate factors $q + \tau^{p^{nt}} l$ and hence of a function of degree t in q and l with coefficients in the $GF[p^n]$.

Theorem. *Any integral invariant with coefficients in the $GF[p^n]$ of the binary group G is an integral function of Q and L with coefficients in the $GF[p^n]$.*

6. The transformation which leaves y unaltered and replaces x by Dx, where $D^s = 1$, leaves Q unaltered and replaces L by DL. Hence Q is an absolute invariant and L a relative invariant of weight unity under the group G' of all binary transformations in the $GF[p^n]$. Hence *any absolute invariant of G' is expressible in terms of Q and L^s, where $s = p^n - 1$.*

The invariants π_m $(m > 2)$ investigated in § 7 are absolute invariants under G' which vanish for no special points. Hence they are expressible in terms of invariants (6) in such a manner that, for $p > 2$, l occurs only to even powers, and in view of the homogenity q occurs only to even powers. Hence, for any p, they are expressible in terms of J and K, where

$$J = Q^{p^n+1}, \qquad K = L^{sp^n}. \tag{7}$$

The Invariants π_m as Functions of the Fundamental Invariants, §§ 7–9.

7. For $m > 1$, let π_m denote the product of all binary forms of degree m which are irreducible in the $GF[p^n]$ and have unity as the coefficient of x^m. Let

$$m = q_1^{r_1} q_2^{r_2} \cdots q_\mu^{r_\mu}, \tag{8}$$

where $q_1, \cdots, q_\mu$ are the distinct prime factors > 1 of m. Set

$$F_t = \frac{x^{p^{nt}-1} - y^{p^{nt}-1}}{x^s - y^s} \qquad (s = p^n - 1). \tag{9}$$

Thus $F_1 = 1$, $F_2 = Q$. It follows readily from *Linear Groups*, page 18, that

$$\pi_m = \frac{F_m \Pi F_{m/q_i q_j} \Pi F_{m/q_i q_j q_k} \cdots}{\Pi F_{m/q_i} \Pi F_{m/q_i q_j q_k} \cdots}, \tag{10}$$

in which the first product in the numerator extends over the $\frac{1}{2}\mu(\mu-1)$ combinations of $q_1, \cdots, q_\mu$ two at a time, and similarly for the remaining products. By § 6, $\pi_m (m>2)$ is an integral function of J and K of degree

$$d_m = \frac{p^{nm} - \sum p^{\frac{nm}{q_i}} + \sum p^{\frac{nm}{q_i q_j}} - \sum p^{\frac{nm}{q_i q_j q_k}} + \cdots}{p^n(p^{2n}-1)}, \tag{11}$$

For example, if m is an odd prime,

$$\pi_m = F_m, \; d_m = \frac{p^{n(m-1)}-1}{p^{2n}-1} \qquad (m \text{ an odd prime}). \tag{12}$$

8. Since $d_3 = 1$, $\pi_3 = F_3$ is a linear function of J and K. By (3),

$$Q^{p^n} = \sum_{k=0}^{p^n} x^{sp^n(p^n-k)} y^{sk p^n}.$$

Hence by (5),

$$J = \sum_{j,\,k=0}^{p^n} x^{s(p^{2n}+p^n-t)} y^{st} \qquad (t = kp^n + j). \tag{13}$$

The terms of (13) given by $j = p^n$ and $k < p^n$ are

$$\sum_{k=0}^{s} x^{s(p^{2n}-kp^n)} y^{sp^n(1+k)} = \sum_{k=0}^{s} x^{p^{2n}(s-k)+kp^n} y^{kp^{2n}+p^n(s-k)}.$$

But every coefficient in the expansion of $(a-b)^s$ is congruent to unity modulo p. Hence the preceding sum equals, in the field,

$$(x^{p^n} y^{p^n} - x^{p^n} y^{p^{2n}})^s = (L^{p^n})^s = K. \tag{14}$$

Next the terms of (13) with $k = p^n$ are

$$\sum_{j=0}^{p^n} x^{s(p^n-j)} y^{s(p^{2n}+j)} = \sum_{\tau=p^{2n}}^{p^{2n}+p^n} x^{s(p^{2n}+p^n-\tau)} y^{s\tau}.$$

When the last sum is combined with the terms of (13) given by $j < p^n$, $k < p^n$, and hence by $t = 0, 1, \cdots, p^{2n}-1$, we get

$$\sum_{t=0}^{p^{2n}+p^n} x^{s(p^{2n}+p^n-t)} y^{st} = \frac{x^{sp^{3n}-1} - y^{sp^{3n}-1}}{x^s - y^s} = F_3.$$

It follows that $\pi_3 = J - K$.

9. We make use of the following identity:

$$(x^{sp^n} - y^{sp^n})(x^{tp^n-1} - y^{tp^n-1}) = (x^{p^{2n}-1} - y^{p^{2n}-1})(x^{tp^n-p^n} - y^{tp^n-p^n}) - (xy)^{sp^n}(x^s - y^s)(x^{tp^n-p^{2n}} - y^{tp^n-p^n}),$$

where $s = p_n - 1$. We divide by $(x^s - y^s)(x^{sp^n} - y^{sp^n})$ and insert the factor $x^{sp^{2n}} - y^{sp^{2n}}$ in the numerator and denominator of the last term. By (14),

$$\frac{(xy)^{sp^n}(x^{sp^{2n}} - y^{sp^{2n}})}{x^{sp^n} - y^{sp^n}} = (xy)^{sp^n}(x^{sp^n} - y^{sp^n})^{p^n-1} = (x^{p^{2n}}y^{p^n} - x^{p^n}y^{p^{2n}})^s = K.$$

Hence we obtain the recursion formula

$$F_t = QF_{t-1}^{p^n} - KF_{t-2}^{p^{2n}} \qquad (F_1 = 1,\ F_2 = Q). \tag{15}$$

Taking $t = 3$ and applying (7) and (12), we get

$$\pi_3 = F_3 = J - K, \tag{16}$$

in agreement with § 8. By (10) and (15) for $t = 4$,

$$\pi_4 = F_4 / Q, \qquad F_4 = QF_3^{p^n} - KQ^{p^{2n}}.$$

Applying (16) and (7) we get

$$\pi_4 = J^{p^n} - J^{p^n-1}K - K^{p^n}. \tag{17}$$

In a similar manner,

$$\pi_5 = J^{p^{2n}+1} - J^{p^{2n}}K - J^{p^{2n}-p^n+1}K^{p^n} - JK^{p^{2n}} + K^{p^{2n}+1}, \tag{18}$$

$$\pi_6 = J^{p^{2n}+p^n-1} - J^{p^{2n}-p^{2n}+p^n-1}K^{p^{2n}} - J^{p^n-1}K^{p^{3n}} - K^{p^n}\left(\frac{J^{p^{2n}} - K^{p^{2n}}}{J - K}\right), \tag{19}$$

$$\pi_7 = J^{p^{2n}-p^n+1}(J^{p^n} - K^{p^n})(J^{p^{4n}} - J^{p^{4n}-p^{3n}}K^{p^{3n}} - K^{p^{4n}}) - JK^{p^{2n}}(J^{p^{4n}} - K^{p^{4n}}) - K\pi_5^{p^{2n}}. \tag{20}$$

The Number of Classes of Irreducible Forms of Degree m, §§ 10–17.

10. Let $\phi(x, y) = x^m + \cdots$ be an irreducible binary form in the $GF[p^n]$. Let $\phi_1 = \phi, \phi_2, \cdots, \phi_k$ be the distinct forms having unity as the coefficient of x^m which are equivalent to a constant multiple of ϕ under the group G of determinant unity. By § 4, the product $P_m = \phi_1 \cdots \phi_k$ is an absolute invariant of G. By § 5, if $m > 2$, P_m is an integral function with coefficients in the $GF[p^n]$ of the invariants q and l, defined by (6). The function $P_m(q, l)$ is obviously irreducible in the field.

Two binary forms shall be said to belong to the same class if and only if one of them is equivalent to a constant multiple of the other under the group G of all binary transformations in the $GF[p^n]$ of determinant unity.

The preceding remarks lead to the

Theorem. *There are as many classes of irreducible binary forms of degree m as there are irreducible factors in the $GF[p^n]$ of the invariant $\pi_m(q, l)$.*

To decide whether or not two given forms ϕ and ψ belong to the same class, we employ a root $\rho = x/y$ of $\phi = 0$ and a root $\sigma = x/y$ of $\psi = 0$, each belonging to the $GF[p^{nm}]$, and determine the values of q/l for $x/y = \rho$ and σ, respectively. According as these values of q/l are the roots of the same factor or different irreducible factors of $\pi_m(q, l)$, the given forms ϕ and ψ belong to the same or different classes.

Since these values of q/l belong to the $GF[p^{nm}]$, *the irreducible factors of* $\pi_m(q, l)$ *are of degree* m *or a divisor of* m.

11. We proceed to the investigation of the irreducible factors of the function $\pi_m(J, K)$ when $p = 2$, and those of this function with J and K replaced by q^2 and l^2 when $p > 2$.

From (16) we conclude that *the cubic forms fall into a single class if* $p = 2$, *and into two classes if* $p > 2$.

For $m = 4$, set $K = \rho J$ in (17). Thus π_4 vanishes only if

$$\rho^{p^n} = 1 - \rho.$$

Then ρ belongs to the $GF[p^{2n}]$ since

$$\rho^{p^{2n}} = 1 - \rho^{p^n} = \rho.$$

For $p = 2$, ρ does not belong to the $GF[2^n]$. Hence π_4 is the product of 2^{n-1} irreducible quadratic factors

$$(K - \rho J)(K - \rho^{p^n} J) = K^2 - KJ + tJ^2,$$

where

$$t = \rho^{p^n+1} = \rho - \rho^2. \tag{21}$$

Hence,* for $p = 2$, t must be a root of

$$t + t^2 + t^4 \cdots + t^{2^{n-1}} = 1. \tag{22}$$

The latter has 2^{n-1} roots in the $GF[2^n]$. Thus, *for* $p = 2$, *the quartic forms fall into* 2^{n-1} *classes differentiated by the roots of* (22).

Next, let $p > 2$. The only value of ρ in the $GF[p^n]$ is $\rho = \frac{1}{2}$. The corresponding factor $q^2 - 2l^2$ is reducible if $p^n = 8l \pm 1$, irreducible if $p^n = 8l \pm 3$. For the remaining $p^n - 1$ values of ρ, $\rho^2 - \rho + t$ is irreducible, so that t has the $\frac{1}{2}(p^n - 1)$ values in the $GF[p^n]$ for which $1 - 4t$ is a not-square. For $l/q = \lambda$, we have $\lambda^2 = \rho$. Now λ will belong to the $GF[p^n]$ only when ρ is a square in the latter field and hence, by (21), only when

$$t^{(p^n-1)/2} = \rho^{(p^{2n}-1)/2} = 1.$$

* In accord with *Linear Groups*, p. 29, formula (23) for $\lambda = \nu = 1$, $p = 2$.

The condition is therefore that t be a square in the $GF[p^n]$. The number of squares t for which $1-4t$ is a not-square is $\frac{1}{4}(p^n-1)$ or $\frac{1}{4}(p^n-3)$ according as -1 is a square or a not-square. Indeed,* $1-\xi^2=\mu\eta^2$, where μ is a not-square, has $p^n\pm 1$ sets of solutions according as -1 is a square or a not-square. The sets $\xi=\pm 1, \eta=0$ are here excluded. We have now shown that, when t has any one of the $\frac{1}{2}(p^n-1)$ values for which $\rho^2-\rho+t$ is irreducible in the $GF[p^n]$, $f(\lambda)=\lambda^4-\lambda^2+t$ is irreducible when t is a not-square, but is reducible when t is a square. In the latter case, set $t=\tau^2$. Then the factors of $f(\lambda)$ are

$$\lambda^2\pm\lambda\sqrt{1+2\tau}+\tau, \tag{23}$$

where τ is that square root of t for which $1+2\tau$ is a square. A partial summary of our results for $p>2$ is given in the following table giving the number of irreducible factors of $\pi_4(q,l)$:

p^n	linear	quadratic	quartic	total number
$8k+1$	2	$\frac{1}{2}(p^n-1)$	$\frac{1}{4}(p^n-1)$	$\frac{1}{4}(3p^n+5)$
$8k-1$	2	$\frac{1}{2}(p^n-3)$	$\frac{1}{4}(p^n+1)$	$\frac{1}{4}(3p^n+3)$
$8k+3$	0	$\frac{1}{2}(p^n-1)$	$\frac{1}{4}(p^n+1)$	$\frac{1}{4}(3p^n-1)$
$8k-3$	0	$\frac{1}{2}(p^n+1)$	$\frac{1}{4}(p^n-1)$	$\frac{1}{4}(3p^n+1)$.

In the following examples we give all the irreducible factors:

$p^n=3$. $\quad q^2-2l^2, \quad l^4-l^2q^2-q^4$.

$p^n=5$. $\quad q^2-2l^2, \quad l^2\pm 2lq-q^2, \quad l^4-l^2q^2+2q^4$.

$p^n=7$. $\quad q\pm 3l, \quad l^2\pm 2lq-2q^2, \quad l^4-l^2q^2+tq^4 \quad (t=3,6)$.

$p^n=9, i^2\equiv i+1 \pmod 3$. $\quad q\pm(i+1)l, \quad l^2\pm ilq-iq^2, \quad l^2\pm(2i+1)lq-(2i+1)q^2,$
$l^4-l^2q^2+tq^4 \quad (t=i, 2i+1)$.

$p^n=11$. $\quad q^2-2l^2, \quad l^2\pm 5lq+q^2, \quad l^2\pm 4lq+2q^2,$
$l^4-l^2q^2+tq^4 \quad (t=6,7,8)$.

For $p>2$, the irreducible quartic forms fall into $6k+2$, $6k$, $6k+2$, or $6k-2$ classes, according as $p^n=8k+1$, $8k-1$, $8k+3$, or $8k-3$, respectively.

Classes of Irreducible Quintic Forms.

12. For quintic forms, (18) vanishes for $K=\rho J$ if

$$\rho^{p^{2n}+1}-\rho^{p^{2n}}-\rho^{p^n}-\rho+1=0. \tag{24}$$

* *Linear Groups*, page 46.

As remarked at the end of § 10, each root of (24) belongs to the $GF[p^{5n}]$. We may give a direct proof as follows.

$$\rho^{p^{2n}} = 1 + \frac{\rho^{p^n}}{\rho - 1}, \qquad \rho^{p^{3n}} = 1 + \frac{1}{\rho - 1} + \frac{\rho}{(\rho - 1)(\rho^{p^n} - 1)},$$

$$\rho^{p^{4n}} = 1 + \frac{\rho}{\rho^{p^n} - 1}, \quad \rho^{p^{5n}} = 1 + \frac{\rho^{p^n}}{\rho^{p^n}/(\rho - 1)} = \rho.$$

If a root of (24) belongs to the $GF[p^n]$, it satisfies the equation

$$\rho^2 - 3\rho + 1 = 0. \tag{25}$$

For $p = 2$, a root of (25) satisfies the equation $\rho^3 \equiv 1$ and hence belongs to the $GF[2^n]$ if and only if n is even. *If $p = 2$, the quintic forms fall into $\frac{1}{5}(2^{2n} + 1)$ or $2 + \frac{1}{5}(2^{2n} - 1)$ classes, according as n is odd or even.* For example, the 6 irreducible quintic forms in the $GF[2]$ are equivalent.

For $p > 2$, we must consider (24) for ρ replaced by λ^2. By § 10, the resulting equation for λ has all its roots in the $GF[p^{5n}]$. If one of its roots belongs to the $GF[p^n]$, it must satisfy the equation

$$\lambda^4 - 3\lambda^2 + 1 = (\lambda^2 + \lambda - 1)(\lambda^2 - \lambda - 1) = 0. \tag{25'}$$

Hence $(2\lambda \pm 1)^2 = 5$, so that $p = 5$ or $p^n = 5k \pm 1$. In the respective cases, we obtain the factors $l \pm 2q$ or

$$l + \tfrac{1}{2}(1 \pm \sqrt{5})q, \qquad l - \tfrac{1}{2}(1 \pm \sqrt{5})q.$$

Hence, if $p > 2$, the irreducible factors are of the following types:

p^n	linear	quintic
5^n	2	$2 \cdot 5^{2n-1}$
$5k \pm 1$	4	$\frac{2}{5}(p^{2n} - 1)$
$5k \pm 2$	0	$\frac{2}{5}(p^{2n} + 1)$

For example, if $p^n = 3$, the factors are

$$\lambda^5 - \lambda^4 - \lambda^3 + \lambda^2 + 1, \ \lambda^5 + \lambda^4 - \lambda^3 - \lambda^2 - 1, \ \lambda^5 - \lambda^4 + 1, \ \lambda^5 + \lambda^4 - 1.$$

For $p > 2$, the irreducible quintic forms fall into

$$2(5^{2n-1} + 1), \ 4 + \tfrac{2}{5}(p^{2n} - 1), \ \tfrac{2}{5}(p^{2n} + 1)$$

classes, according as $p = 5$, $p^n = 5k \pm 1$, or $p^n = 5k \pm 2$.

Classes of Irreducible Sextic Forms.

13. For sextic forms, (19) vanishes for $K = \rho J$ if

$$1-\rho^{p^{2n}}-\rho^{p^{3n}}-\rho^{p^{2n}}\left(\frac{1-\rho^{p^n}}{1-\rho}\right)=0. \tag{26}$$

For $\rho=1$ the final term is a multiple of p, so that $\rho=1$ is not a root. For $p=2$ or $p=3$, there is no root in the $GF[p^n]$, while for $p>3$, the only root is $\rho=\frac{1}{3}$.

We determine the roots of (26) which belong to the $GF[p^{2n}]$ by a simple device. Any such root satisfies the equation

$$1-\rho-\rho^{p^n}=\rho^{p^n}\left(\frac{1-\rho^{p^n}}{1-\rho}\right). \tag{27}$$

The first member equals its p^n-th power. Hence

$$\rho^n=1-\rho-s, \tag{28}$$

where s is an element of the $GF[p^n]$. Hence (27) gives

$$s=\frac{(1-\rho-s)(\rho+s)}{1-\rho}$$

$$\rho^2+\rho(s-1)+s^2=0. \tag{29}$$

Hence any root of (26) which belongs to the $GF[p^{2n}]$, but not to the $GF[p^n]$, satisfies an equation of type (29) irreducible in the $GF[p^n]$. Conversely, any root ρ of an irreducible equation (29) is a root of (26). Indeed, the second root is ρ^{p^n} and the sum of the roots is $1-s$; thus (28) and hence also (27) is satisfied. Now, for $p>2$, (29) is irreducible if and only if $(1+s)(1-3s)$ is a not-square in the $GF[p^n]$. We readily verify* that this is the case for the following number of values of s:

$$\tfrac{1}{2}(p^n-3) \text{ if } p^n=3l+2, \qquad \tfrac{1}{2}(p^n-1) \text{ if } p=3 \text{ or } p^n=3l+1. \tag{30}$$

For $p>2$, we must investigate the reducibility of (29) when ρ is replaced by λ^2. By the product of the roots,

$$\rho^{p^n+1}=s^2, \qquad \rho^{(p^{2n}-1)/2}=+1,$$

so that ρ is a square in the $GF[p^{2n}]$. Hence the quartic in λ is reducible. Its factors are

$$\lambda^2+a\lambda\pm s, \qquad \lambda^2-a\lambda\pm s,$$

where $a^2=1-s\pm 2s$. The product of the two values for a^2 is the not-square $(1+s)(1-3s)$, so that one value is a square.

* By means of *Linear Groups*, p. 48, § 66. Note that -3 is a square or not-square according as $p^n=3l+1$ or $3l+2$.

Examples. If $p^n = 3$, then $s = 1$ and

$$\lambda^4 + 1 = (\lambda^2 + \lambda - 1)(\lambda^2 - \lambda - 1).$$

If $p^n = 5$, then $s = -2$, and

$$\lambda^4 + 2\lambda^2 - 1 = (\lambda^2 + 2\lambda - 2)(\lambda^2 - 2\lambda - 2).$$

If $p = 2$, we multiply (29) by $(s-1)^{-2}$ and set

$$\sigma = \rho(s-1)^{-1}, \qquad t = s^2(s^2+1)^{-1}.$$

Then $\sigma^2 + \sigma + t = 0$. This is irreducible if and only if t is one of the 2^{n-1} roots of (22) in the $GF[2^n]$. Unless $t = 1$, the corresponding value of s is uniquely determined in the field. But $t = 1$ is a root of (22) if and only if n is odd. Hence the number of values of s for which (29) is irreducible in the $GF[2^n]$ is

(31) $\qquad 2^{n-1} - 1$ for n odd, $\qquad 2^{n-1}$ for n even.

The number is zero for $n = 1$: for $n = 2, 3, 4$, s is a root of

$$s^2 + s + 1 = 0, \qquad s^3 + s + 1 = 0, \qquad (s^4 + s + 1)(s^4 + s^3 + 1) = 0.$$

It remains to determine the roots of (26) which belong to the $GF[p^{3n}]$. These must satisfy the equation

$$\rho + \rho^{p^n} + \rho^{p^{2n}} = 1. \tag{32}$$

Conversely, any root of the latter belongs to the $GF[p^{3n}]$ and, with the exception of $\rho = 1$ when $p = 2$, satisfies (26). A root of (32) belongs to the $GF[p^n]$ only when $3\rho = 1$. Hence the irreducible cubic factors of (26) are of the form $\rho^3 - \rho^2 + \cdots$ and their number is

(33) $\qquad 3^{2n-1}$ if $p = 3$, $\qquad \frac{1}{3}(p^{2n} - 1)$ if $p \neq 3$.

By § 15, these factors give all the existing irreducible cubics $x^3 - x^2 + \cdots$.

The irreducible factors of (26) are of degree 6 or a divisor of 6. Denote by L, Q, C the number of linear, quadratic and cubic factors, respectively. Then the number of degree 6 is

$$S = \tfrac{1}{6}(p^{3n} + p^n - 1 - L - 2Q - 3C).$$

By the above results we have, whether $p = 2$ or $p > 2$,

$$\begin{aligned} &S = \tfrac{1}{6}(p^{3n} - p^{2n} + 2) \text{ for } p^n = 3l + 2, \\ &S = \tfrac{1}{6}(p^{3n} - p^{2n}) \text{ for } p = 3 \text{ or } p^n = 3l + 1. \end{aligned} \tag{34}$$

In view of (31), (33), (34), we have the

Theorem. *If $p=2$, the number of classes of irreducible sextic forms is $\frac{1}{6}(2^{3n}+2^{2n}+3\cdot 2^n-6)$ for n odd, $\frac{1}{6}(2^{3n}+2^{2n}+3\cdot 2^n-2)$ for n even.*

For $p^n=2$ this number is 2. The irreducible factors of (26) are then

$$\rho^3+\rho^2+1, \qquad \rho^6+\rho^5+1.$$

Irreducible Cubics whose Roots are Squares with a given Sum.

14. For sextic forms when $p>2$ there remains the difficult problem: to determine which of the cubics

$$C=\rho^3-\rho^2+a\rho-b \tag{35}$$

are irreducible and give irreducible sextics when ρ is replaced by λ^2, and which give reducible sextics. The first or second case arises according as ρ is a not-square or a square in the $GF[p^{3n}]$, namely, according as b is a not-square or a square in the $GF[p^n]$. In fact,

$$b=\rho\cdot\rho^{p^n}\cdot\rho^{p^{2n}}, \qquad b^{(p^n-1)/2}=\rho^{(p^{3n}-1)/2}.$$

In the second case, $b=e^2$, and $\lambda^6-\lambda^4+a\lambda^2-e^2$ has the factors

$$\lambda^3\pm c\lambda^2+\tfrac{1}{2}(c^2-1)\lambda\pm e, \tag{36}$$

where

$$c^4-2c^2-8ec+1-4a=0.$$

This quartic has the resolvent cubic

$$y^3+2y^2-4(1-4a)y-8(1-4a)-64e^2=0.$$

We set $y=2z$ and multiply the resulting equation by 8, and get

$$z^3+z^2+(4a-1)z-1+4a+8b=0.$$

If in the cubic $8C=0$ we replace ρ by $\frac{1}{2}(z+1)$, we obtain the preceding cubic. Hence the resolvent cubic is irreducible, so that* the quartic has one and but one root c in the $GF[p^n]$. The unique pair of factors of the sextic in λ are therefore of the form (36).

To determine the irreducible cubics (35) in which $b=e^2$,

$$C=\rho^3-\rho^2+a\rho-e^2 \qquad (e\neq 0), \tag{37}$$

we proceed indirectly and find those which are reducible.

(*a*) First, let C have a linear factor $\rho-k$ and an irreducible quadratic factor. The latter must be of the form $\rho^2+(k-1)\rho+ks^2$, where $s^2=e^2/k^2\neq 0$.

* Bulletin of the American Mathematical Society, vol. 13 (1906), p. 5, middle of p. 7.

The quadratic is irreducible if and only if $(k-1)^2-4ks^2$ is a not-square. Let ν be a fixed not-square and let $p^n=4l\pm1$, the upper or lower sign holding according as -1 is a square or a not-square. Then

$$(k-1)^2-4ks^2=\nu z^2$$

has $p^n\mp1$ sets of solutions s, z when k is any chosen not-square, $p^n\pm1$ sets when k is any chosen square $\neq1$, while for $k=0$ or 1 the solutions are obvious. After excluding the sets in which either $s=0$ or $z=0$, and dividing by 4, we obtain the number of values of $s^2\neq0$ for which $(k-1)^2-4ks^2$ is a not-square. If -1 is a square the number of sets s^2, k, and hence the number of irreducible quadratics, is

$$\tfrac{1}{4}(p^n-1)\cdot\tfrac{1}{2}(p^n-1)+\tfrac{1}{4}(p^n-1)\cdot\tfrac{1}{2}(p^n-3)=\tfrac{1}{4}(p^n-1)(p^n-2).$$

If -1 is a not-square, the number is

$$\tfrac{1}{4}(p^n+1)\cdot\tfrac{1}{2}(p^n-1)+\tfrac{1}{4}(p^n-3)\cdot\tfrac{1}{2}(p^n-3)+\tfrac{1}{2}(p^n-1)=\tfrac{1}{2}(p^{2n}-p^n+2).$$

In the following examples we give all the irreducible quadratics: For $p^n=3$, $s^2=1$, $k=\pm1$. For $p^n=5$, $s^2=1$, $k=2, 3, 4$. For $p^n=7$, $s^2=1$, $k=1, 3, 5$; $s^2=2$, $k=1, 2, 4, 6$; $s^2=4$, $k=1, 3, 5, 6$. For $p^n=11$, $s^2=1$, $k=1, 5, 7, 8, 9, 10$; $s^2=3$, $k=1, 2, 6, 7, 8$; $s^2=4$, $k=1, 2, 5, 6, 9$; $s^2=5$, $k=1, 3, 4, 7, 8, 10$; $s^2=9$, $k=1, 2, 3, 4, 6, 10$. For $p^n=9$, $i^2\equiv-1\pmod3$, $s^2=1$, $k=\pm i+1, \pm i-1$; $s^2=\pm i$, $k=-1, i, -i, \mp i+1, \mp i-1$.

(b) Next let (37) have three roots in the $GF[p^n]$. Either all three are squares or only one root is a square.

(b_1) Let the three roots be squares. We seek the number of systems of three squares s_i with the sum unity, two systems being identified if they are composed of the same s_i in different orders.

If t is the number of systems with $s_1=s_2=s_3$, we have

(38) $\quad t=0$ if $p=3$ or $p^n=12k\pm5$, $\quad t=1$ if $p^n=12k\pm1$.

Let μ be the number of sets with $s_1=s_2$. Now $x^2+2y^2=1$ has p^n-1 or p^n+1 sets of solutions according as -2 is a square or a not-square. Of these, 4 or 2 have $xy=0$, according as 2 is a square or a not-square, namely, according as $p^n=8l\pm1$ or $8l\pm3$. Hence

$$\mu=\tfrac{1}{4}(p^n-5) \text{ if } p^n=8l+1, \quad \tfrac{1}{4}(p^n-3) \text{ if } p^n=8l-1 \text{ or } 8l+3,$$
$$\tfrac{1}{4}(p^n-1) \text{ if } p^n=8l+5.$$

The number of sets s_i in which exactly two are equal is therefore $3(\mu-t)$.

Next, the total number of sets of solutions of *

$$x^2 + y^2 + z^2 = 1$$

is $p^{2n} \pm p^n$ according as $p^n = 4l \pm 1$. These include $p^n \mp 1$ sets with $z = 0$. Hence the numbers of sets of squares s_i whose sum is unity is

$$k = \tfrac{1}{8}\{ p^{2n} \pm p^n - 3(p^n \mp 1 - 4) - 6 \}.$$

Hence there are $\frac{1}{6}\{k - 3(\mu - t) - t\}$ systems in which s_1, s_2, s_3 are all distinct. As shown above, there are $\mu - t$ systems in which exactly two of the s_i are equal, and t systems with all three equal. The total number of systems is therefore $\frac{1}{6}(k + 3\mu + 2t)$.

(b_2) Let one of the roots be a square s and the other two not-squares n_1, n_2. If the latter are equal, we employ the $p^n - 1$ or $p^n + 1$ sets of solutions of $x^2 + 2\nu y^2 = 1$, according as -2 is a not-square or a square, namely, according as $p^n = 8l - 1,\ 8l - 3$ or $p^n = 8l + 1,\ 8l + 3$. Now there are two sets of solutions with $x = 0$ if 2 is a not-square, namely, if $p^n = 8l \pm 3$. Hence the number of sets $s, n_1 = n_2$ is

$$N = \tfrac{1}{4}(p^n - 1) \text{ if } p^n = 8l + 1, \qquad \tfrac{1}{4}(p^n - 3) \text{ if } p^n = 8l - 1 \text{ or } 8l + 3,$$
$$\tfrac{1}{4}(p^n - 5) \text{ if } p^n = 8l + 5.$$

The total number of sets of solutions of $x^2 + \nu y^2 + \nu z^2 = 1$ is $p^{2n} \pm p^n$ according as $p^n = 4l \pm 1$. These include $p^n \mp 1$ sets with $x = 0$ and $p^n \pm 1$ sets with $y = 0$. Hence the total number of sets s, n_1, n_2 is

$$M = \tfrac{1}{8}\{ p^{2n} \pm p^n - (p^n \mp 1) - 2(p^n \pm 1 - 2) - 2 \}.$$

The total number of systems is therefore $\frac{1}{2}(M - N) + N = \frac{1}{2}M + \frac{1}{2}N$. Now

$$\tfrac{1}{6}k + \tfrac{1}{2}M = \tfrac{1}{12}(p^{2n} \pm p^n - 3p^n + 3),$$

while $N + \mu = \frac{1}{2}(p^n - 3)$ for all values of p^n. Hence the number of cubics (37) with three roots in the $GF[p^n]$ is $\frac{1}{12}(p^{2n} \pm p^n - 6) + \frac{1}{3}t$, according as $p^n = 4l \pm 1$.

Combining this number with the number obtained in case (a), we get

$$\tfrac{1}{3}(p^{2n} - 2p^n + t) \text{ if } p^n = 4l + 1, \qquad \tfrac{1}{3}(p^{2n} - p^n + t) \text{ if } p^n = 4l - 1.$$

The total number of cubics (37) is $\frac{1}{2}(p^n - 1)p^n$. Hence, by (38), we obtain the

Theorem. *The number of irreducible cubics* (37) *is*

* *Linear Groups*, p. 48.

$$(39)\qquad \begin{aligned} &\tfrac{1}{6}(p^n \mp 1)(p^n \pm 2) \text{ if } p^n = 12k \pm 1, \\ &\tfrac{1}{6}p^n(p^n \pm 1) \text{ if } p^n = 12k \pm 5, \text{ or if } p = 3 \text{ and } \pm 1 = (-1)^n. \end{aligned}$$

A check upon the above results is afforded by the following examples which give all systems of three elements in the $GF[p^n]$ whose sum is unity and whose product is a square:

$p^n = 3$, none; $p^n = 5$, $1, 1, 4; 1, 2, 3$; $p^n = 7$, $4, 2, 2; 2, 3, 3; 4, 5, 6$;

$p^n = 3^2$, $i^2 \equiv -1 \pmod 3$, $1, 1, 2; i, -i, 1; 1, i \pm 1, -i \mp 1;$

$-1, i+1, -i+1; \pm i, \pm i - 1, \pm i - 1$;

$p^n = 11$, $4, 4, 4; 3, 4, 5; 5, 9, 9; 3, 2, 7; 3, 10, 10;$

$4, 2, 6; 5, 8, 10; 9, 7, 7; 9, 6, 8$;

$p^n = 13$, $1, 1, 12; 1, 3, 10; 1, 4, 9; 3, 12, 12; 9, 9, 9; 1, 2, 11; 1, 5, 8;$

$1, 6, 7; 3, 5, 6; 4, 2, 8; 4, 5, 5; 9, 7, 11; 10, 2, 2; 10, 6, 11; 12, 7, 8.$

By excluding the resulting cubics and those given by the examples under case (a), we find the only irreducible cubics (37) are those in which a, e^2 is one of the following sets:

$p^n = 3$, $2, 1$; $p^n = 5$, $1, -1; 3, -1; 0, 1; 4, 1; 3, 1$;

$p^n = 7$, $0, 1; 3, 1; 5, 1; 1, 2; 5, 2; 2, 4; 5, 4$;

$p^n = 9$, $i^2 \equiv -1 \pmod 3$, $0, -1; 1, -1; \pm i, -1; -1, 1;$

$\pm i + 1, 1; \pm i - 1, 1; 0, \pm i; 1, \pm i; \pm i - 1, \mp i$;

$p^n = 11$, $3, 1; 7, 1; 0, 3; \pm 1, 3; 2, 3; \pm 2, 4; 6, 4; 7, 4;$

$8, 4; 0, 5; 7, 5; 10, 5; 1, 9; 2, 9; 3, 9; 5, 9.$

15. The investigation made in § 14 enables us to determine the number N_{gs} of irreducible cubics $x^3 - gx^2 + hx + k$, in which g is a given element and k ranges over the squares, and the corresponding number N_{gn} when k ranges over the not-squares.

Let C_g be the number of all the irreducible cubics $x^3 - gx^2 + \cdots$ in which g is a given element. If ρ is a root of such a cubic,

$$(40)\qquad \rho + \rho^{p^n} + \rho^{p^{2n}} = g, \qquad \rho^{p^{3n}} = \rho.$$

Since the latter equation follows from the former, we conclude that (40_1) has p^{2n} roots in the $GF[p^{3n}]$. If such an element ρ is distinct from ρ^{p^n} it is a root of a cubic irreducible in the $GF[p^n]$. Now a common root of $\rho = \rho^{p^n}$ and (40_1)

makes $3\rho = g$, so that the two equations have a single solution if $p \neq 3$, no solution if $p = 3$, $g \neq 0$, and 3^n solutions if $p = 3$, $g = 0$. Hence

(41) $C_g = \frac{1}{3}(p^{2n}-1)$ if $p \neq 3$, $C_0 = \frac{1}{3}(3^{2n}-3^n)$ if $p=3$, $C_{g'} = 3^{2n-1}$ if $p=3$, $g' \neq 0$.

For any p, the total number of irreducible cubics is therefore $\frac{1}{3}p^n(p^{2n}-1)$, in agreement with § 7. Conversely, if * $p \neq 3$, the latter result implies (41), since $x' = x + \frac{1}{3}(g+g')$ transforms each $x^3 - gx^2 + \cdots$ into a cubic $x^3 - g'x^2 + \cdots$.

If ν is a fixed not-square in the $GF[p^n]$, (40_1) gives

$$\nu\rho + (\nu\rho)^{p^n} + (\nu\rho)^{p^{2n}} = \nu g.$$

First, let ρ be a square in the $GF[p^{3n}]$. Since ν is a not-square in the $GF[p^{3n}]$, $\nu\rho$ is a not-square. Hence

$$N_{0s} = N_{0n}, \qquad N_{gs} = N_{g'n},$$

where one of the elements g, g' is any square and the other any not-square. Thus *if σ is any square and ν any not-square in the $GF[p^n]$,*

(42) $\quad N_{0s} = N_{0n} = \frac{1}{2}C_0, \qquad N_{\nu n} = N_{\sigma s} = N_{1s}, \qquad N_{\nu s} = N_{\sigma n} = C_1 - N_{1s},$

where C_0 and C_1 are given by (41) *and N_{1s} is given by* (39).

16. We may now enumerate the irreducible factors in the $GF[p^n]$, $p > 2$, of the function of degree $d = 2(p^{3n} + p^n - 1)$ derived from (26) by replacing ρ by λ^2. First, if $p \neq 3$, $\lambda^2 - \frac{1}{3}$ has $t+1$ factors, where t is defined by (38). Next, there are $2r$ further irreducible quadratic factors, where r is defined by (30). Again, there are $2N_{1s}$ irreducible cubic factors and N_{1n} irreducible sextic factors, all derived from the cubic functions of ρ (§ 14). The remaining factors are irreducible sextics; their number is therefore

$$\tfrac{1}{6}(d - e - 4r - 6N_{1s} - 6N_{1n}) \quad (e=0 \text{ if } p=3,\ e=2 \text{ if } p \neq 3).$$

Thus if $\beta = 0$ when $p = 3$, $\beta = t + \frac{2}{3}$ if $p \neq 3$. the total number of factors is

$$\tfrac{1}{6}d + \beta + \tfrac{4}{3}r + N_{1s}.$$

Hence we may state the following

Theorem. *The number of classes of irreducible sextics in the $GF[p^n]$, $p > 2$, is $\frac{1}{6}(2p^{3n} + p^{2n} + 7p^n - a)$, $a = -2$ if $p^n = 12k+1$, $a = 10$ if $p^n = 12k+5$, $a = 6$ if $p = 3$, n even; $\frac{1}{6}(2p^{3n} + p^{2n} + 5p^n - b)$, $b = 2$ if $p^n = 12k-5$, $b = 6$ if $p^n = 12k-1$ or if $p = 3$, n odd.*

* By means of $x' = gx$ we conclude that, for any p, $C_g = C_1$ if $g \neq 0$. The value of C_0 was determined otherwise in Bulletin of the American Mathematical Society, l. c., pp. 3, 4.

For $p^n = 3$, the 12 irreducible factors* are

$$\lambda^2 \pm \lambda - 1,\ \lambda^3 \pm \lambda^2 \mp 1,\ \lambda^6 - \lambda^4 + 1,\ \lambda^6 - \lambda^4 + \lambda^2 + 1,$$
$$\lambda^6 \pm \lambda^5 - \lambda^4 + \lambda^2 - 1,\ \lambda^6 \pm \lambda^5 \pm \lambda^3 - 1,\ \lambda^6 \pm \lambda^5 \mp \lambda^3 + 1.$$

For $p^n = 5$, the 50 irreducible factors are 34 sextics† and

$$\lambda^2 - 2,\ \lambda^2 \pm 2\lambda - 2,\ \lambda^3 \pm \lambda^2 \pm 2,\ \lambda^3 \pm 2\lambda^2 - \lambda \pm 2,\ \lambda^3 \mp 2\lambda^2 - \lambda \pm 1,$$
$$\lambda^3 + 2\lambda \pm 1,\ \lambda^3 \pm \lambda^2 \pm 1,\ \lambda^6 - \lambda^4 - \lambda^2 - 3,\ \lambda^6 - \lambda^4 + \lambda^2 - 3,\ \lambda^6 - \lambda^4 - 2.$$

For $p^n = 7$, the 128 irreducible factors are 98 sextics† and

$$\lambda^2 - 5,\ \lambda^2 \pm 3\lambda + 1,\ \lambda^2 \pm 3\lambda - 2,\ \lambda^2 \pm 2\lambda + 3,\ \lambda^3 \pm 2\lambda^2 - 2\lambda \pm 1,\ \lambda^3 \pm \lambda^2 \pm 1,$$
$$\lambda^3 \pm 3\lambda^2 + 4\lambda \pm 1,\ \lambda^3 \pm \lambda^2 \pm 3,\ \lambda^3 \pm 3\lambda^2 + 4\lambda \pm 3,\ \lambda^3 + 3\lambda \pm 2,\ \lambda^3 \pm 2\lambda^2 - 2\lambda \mp 2,$$
$$\lambda^6 - \lambda^4 + 4\lambda^2 - 6,\ \lambda^6 - \lambda^4 + 6\lambda^2 - 3,\ \lambda^6 - \lambda^4 - 3,\ \lambda^6 - \lambda^4 + \lambda^2 - 5,\ \lambda^6 - \lambda^4 + 5\lambda^2 - 3,$$
$$\lambda^6 - \lambda^4 + 2\lambda^2 - 6,\ \lambda^6 - \lambda^4 + 3\lambda^2 - 5,\ \lambda^6 - \lambda^4 + 4\lambda^2 - 3,\ \lambda^6 - \lambda^4 + 6\lambda^2 - 5.$$

Classes of Irreducible Septic Forms.

17. For septic forms we set $K = \rho J$ in (20) and obtain an equation of degree $d = p^{4n} + p^{2n} + 1$ in ρ, having d roots in the $GF[p^{7n}]$. For $\rho^{p^n} = \rho$, the equation becomes

$$1 - 5\rho + 6\rho^2 - \rho^3 = 0. \tag{43}$$

If $p = 2$, a root of (43) belongs to the exponent 7 and hence belongs to the $GF[2^n]$ if and only if 7 is a divisor of $2^n - 1$, namely, if n is a multiple of 3. In the latter case there are 3 linear and $\frac{1}{7}(d-3)$ irreducible septic factors. But if n is prime to 3, all the factors are septics. For example, if $n = 1$, 2, or 3, the number of septic factors is 3, 39, or 594, respectively. *If $p = 2$, the number of classes of irreducible septic forms is $3 + \frac{1}{7}(d-3)$ or $\frac{1}{7}d$, according as n is a multiple of 3 or prime to 3.*

If we set $\rho = \sigma + 2$ in (43), we get‡

$$\sigma^3 - 7\sigma - 7 = 0. \tag{44}$$

Hence if $p = 7$, $\rho = 2$ is the only root in the $GF[p^n]$. Upon replacing ρ by λ^2 we obtain the linear factors $\lambda \pm 3$ and $\frac{1}{7}(2d-2)$ irreducible septic factors. *For $p = 7$, the number of classes of irreducible septic forms is* $2 \cdot 7^{4n-1} + 2 \cdot 7^{2n-1} + 2$.

* Two factors with an ambiguous sign are obtained from the same irreducible function of ρ.

† The omitted sextics are by pairs factors of an irreducible sextic in $\rho = \lambda^2$.

‡ This cubic is a resolvent for the seventh roots of unity. For its numerical solution see SERRET, *Algèbre Supérieure*, vol. 1, pp. 338, 343.

For $p \neq 2$, $p \neq 7$, we determine the number N of distinct roots of (43) in the $GF[p^n]$ by the following indirect process. Since the equation of degree d has $d - N$ roots in the $GF[p^{7n}]$, not belonging to the $GF[p^n]$, it has

$$E = \tfrac{1}{7}(p^{4n} + p^{2n} + 1 - N)$$

irreducible septic factors. Thus E must be an integer. Since the discriminant of (43) or (44) is the square 7^2, we have $N = 0$ or 3 (Bulletin, l. c., p. 1). Now p^{2n} is of the form $7l + s$, where $s = 1, 2$ or 4. Thus E is an integer only when $N = 3$, 0 or 0, respectively. Hence for $p \neq 2$, $p \neq 7$, the cubic (43) has 3 roots in the $GF[p^n]$ if $p^n = 7k \pm 1$, no root if $p^n = 7k \pm 2, \pm 3$. In the former case, each root r is a square in the $GF[p^n]$; for, if not, each root of $\lambda^2 = r$ would belong to the $GF[p^{2n}]$ and not to the $GF[p^n]$, whereas all the roots of the λ-equation belonging to the $GF[p^{7n}]$. Hence if $p^n = 7k \pm 1$, $p > 2$, there are six linear factors. For example,

$$p^n = 13,\ \lambda \pm 2,\ \lambda \pm 4,\ \lambda \pm 8; \quad p^n = 29,\ \lambda \pm 4,\ \lambda \pm 8,\ \lambda \pm 10;$$

$$p^n = 41,\ \lambda \pm 3,\ \lambda \pm 10,\ \lambda \pm 15; \quad p^n = 43,\ \lambda \pm 9,\ \lambda \pm 16,\ \lambda \pm 20.$$

For $p \neq 2$, $p \neq 7$, the number of classes of irreducible septics is

$$6 + \tfrac{2}{7}(p^{4n} + p^{2n} - 2) \text{ or } \tfrac{2}{7}(p^{4n} + p^{2n} + 1),$$

according as p^n is or is not of the form $7k \pm 1$.

THE UNIVERSITY OF CHICAGO,
July 14, 1910.

AN APPLICATION OF SYMBOLIC METHODS TO THE TREATMENT OF MEAN CURVATURES IN HYPERSPACE*

BY

WILLIAM HUNT BATES

This paper is an application of MASCHKE's symbolic method for discussing invariants of quadratic differential forms, as developed in his article, *A Symbolic Treatment of the Theory of Invariants of Quadratic Differential Quantics of n Variables.*† Extensive use is also made of results and methods contained in two later publications, *Differential Parameters of the First Order*,‡ and *The Kronecker-Gaussian Curvature of Hyperspace.* § Some familiarity with these three articles is implied.

Part I of the present paper is devoted to the study of the curvatures of an n-space R_n in an euclidean $(n+1)$-space S_{n+1}. In §§ 1–3 the equations and some of the properties of the lines of curvature of R_n in S_{n+1} are developed. In particular, equation (28) gives the n curvatures of the n lines of curvature through a given point of R_n. The coefficients $K_1, \cdots, K_n$ of this equation are the so-called curvatures of R_n in S_{n+1}, involving the coefficients a_{ik} and α_{ik} of the two fundamental forms of R_n. With the help of his symbolic method, ‖ MASCHKE has expressed K_n, when n is even, and K_n^2, when n is odd, as rational integral functions of the coefficients a_{ik} of the first fundamental form and their derivatives.

In §§ 4–6 similar expressions are derived for all the curvatures $K_{2\nu}$ of even index. It does not seem possible to obtain rational results for the curvatures $K_{2\nu+1}$ of odd index. In § 7, however, it is shown that, with the exception of K_1, these curvatures are expressible irrationally in terms of the first fundamental quantities and their derivatives.

The symbolic expressions for $K_{2\nu}$ and K_n^2 show at once that they are differential invariants of the first fundamental quadratic form for R_n, and they have meaning as invariants of any quadratic form in n variables. Part II of this paper considers a space R_λ defined in a space $R_n (n > \lambda)$, which is not neces-

* Presented to the Society December 31, 1910.

† These Transactions, vol. 4 (1903), pp. 445–469. This paper is referred to hereafter as M. I.

‡ *Ibid.*, vol. 7 (1906), pp. 69–80; referred to as D. P.

§ *Ibid.*, vol. 7 (1906), pp. 81–93; referred to as K.-G. C.

‖ In K.-G. C.

sarily euclidean. The invariants $K_{2\nu}$ and K_λ^2 for R_λ are calculated in terms of the coefficients a_{ik} belonging to the length element of R_n and of the functions $U^{\lambda+1}, \cdots, U^n$ which determine the space R_λ in R_n.

PART I.

CURVATURES OF AN n-SPACE IN AN $(n+1)$-SPACE.

§ 1. *Parametric Representation for an n-space in an $(n+1)$-space.*

Let $z', z^2, \cdots, z^{n+1}$ be the coördinates* of an euclidean space S_{n+1} of $n+1$ dimensions, i. e., a space whose arc-element is of the form

$$ds^2 = \sum_{i=1}^{n+1} [dz^i]^2. \tag{1}$$

We define in S_{n+1} any hypersurface, or space R_n, of n dimensions, by expressing each z as a funcion of n independent variables $x_1, \cdots, x_n$:

$$\begin{aligned} z' &= z'(x_1, \cdots, x_n), \\ &\cdots\cdots\cdots\cdots \\ z^{n+1} &= z^{n+1}(x_1, \cdots, x_n). \end{aligned} \tag{2}$$

The arc-element of R_n is given by the equation

$$ds^2 = \sum_{i,k}^{1,\cdots,n} a_{ik}\, dx_i\, dx_k, \tag{3}$$

where

$$a_{ik} = \sum_{j=1}^{n+1} \frac{\partial z^j}{\partial x_i}\frac{\partial z^j}{\partial x_k} = \sum_{j=1}^{n+1} z_i^j z_k^j = f_i f_k, \tag{4}$$

differentiation with respect to x_i being indicated here, as in the following pages, by the lower index i.

A space of λ dimensions, $\lambda < n$, would be obtained by using in (2) only λ independent variables $x_1, \cdots, x_\lambda$. In particular, a curve in S_{n+1} is obtained by expressing each z as a function of one new variable x.

If in (2) one puts $x_2 = \cdots = x_n = 0$, the resulting curve is called the x_1-axis of a curvilinear system of coördinates on R_n. By letting $x_2, \cdots, x_n$ represent arbitrary constants, one gets the complete system of x_1-curves; and similarly for the other cases.

$$\begin{aligned} &x_1\text{-curves if } x_1 \text{ varies and } x_2, \cdots, x_n \text{ are constants}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &x_n\text{-curves if } x_n \text{ varies and } x_1, \cdots, x_{n-1} \text{ are constants}. \end{aligned} \tag{5}$$

Equations (3) and (5) give the elements of the new axes,

$$ds_1^2 = a_{11}\, dx_1^2, \cdots, ds_n^2 = a_{nn}\, dx_n^2, \tag{6}$$

* It is assumed that no confusion will arise from writing the upper index, as MASCHKE does, without parentheses. Exponents are only occasionally used, and will be easily recognized.

where ds_k is the element of the x_k-axis. Represent the direction cosines of the x_k-axis, in the old system, by $\cos(z', x_k), \cdots, \cos(z^{n+1}, x_k)$. Then

$$(7) \qquad \cos(z^j, x_k) = \frac{dz^j}{ds_k} = \frac{z_\alpha^j dx_k}{\sqrt{a_{kk}}\, dx_k} = \frac{z_k^j}{\sqrt{a_{kk}}} \quad (j=1, \cdots, n+1; k=1, \cdots, n).$$

Let ω_{ik} be the angle between the x_i-axis and the x_k-axis. Then

$$(8) \quad \cos\omega_{ik} = \sum_{j=1}^{n+1} \cos(z^j x_i)\cos(z^j x_k) = \sum_{j=1}^{n+1} \frac{z_i^j z_k^j}{\sqrt{a_{ii}}\sqrt{a_{kk}}} = \frac{a_{ik}}{\sqrt{a_{ii}}\sqrt{a_{kk}}} \quad (i, k=1, \cdots, n),$$

so that *necessary and sufficient conditions for mutual orthogonality of the axes of the new system are*

$$(9) \qquad a_{ik} = 0 \qquad (i, k=1, \cdots, n;\ i \neq k).$$

§ 2. *General Curves on R_n.*

A general curve on R_n may be defined by means of $n-1$ equations,

$$(10) \qquad U^2(x_1, \cdots, x_n) = \text{const.}, \cdots, U^n(x_1, \cdots, x_n) = \text{const.}$$

The differential equations of this curve, which we call the U-curve, are

$$(11) \qquad \sum_{i=1}^{n} U_i^2 dx_i = 0, \cdots, \sum_{i=1}^{n} U_i^n dx_i = 0.$$

Its direction is defined by the ratios of $dx_1, \cdots, dx_n$ in (11). In order to solve for these differentials, let p be any function of $x_1, \cdots, x_n$ which satisfies the condition *

$$D = (pU^2 \cdots U^n) = (pU) \neq 0.$$

If A^r denotes the cofactor of p_r in D, equations (11) are identically satisfied by

$$(12) \qquad dx_1 = \rho A', \cdots, dx_n = \rho A^n,$$

where ρ is an arbitrary parameter.

The direction cosines $\xi', \cdots, \xi^{n+1}$ of the U-curve are found as follows. From (12),

$$(13) \qquad \sum_{i=1}^{n} p_i dx_i = \rho \sum_{i=1}^{n} p_i A^i = \rho(pU).$$

Then

$$\xi^k = \frac{dz^k}{ds} = \frac{1}{ds}\sum_{i=1}^{n} z_i^k dx_i = \frac{\rho}{ds}(z^k U),$$

where ds is arc-element of the U-curve. Now

$$\sum_{k=1}^{n} [\xi^k]^2 = 1 = \sum_{k=1}^{n+1} \left[\frac{\rho}{ds}\right]^2 (z^k U)^2 = \left[\frac{\rho}{ds}\right]^2 (fU)^2.$$

* See M. I., § 2, for an explanation of this invariantive notation.

Hence

$$\frac{\rho}{ds} = \frac{1}{\sqrt{(fU)^2}}.$$

Then the direction cosines of the U-curve on R_n, referred to the original system of axes, are

$$\xi' = \frac{(z'U)}{\sqrt{(fU)^2}}, \quad \cdots, \quad \xi^{n+1} = \frac{(z^{n+1}U)}{\sqrt{(fU)^2}}. \tag{14}$$

If there is given also a V-curve on R_n by equations similar to (10), its direction cosines may be written

$$\eta' = \frac{(z'V)}{\sqrt{(fV)^2}}, \quad \cdots, \quad \eta^{n+1} = \frac{(z^{n+1}V)}{\sqrt{(fV)^2}}. \tag{15}$$

If ω is the angle between the two curves, we have from (14) and (15)

$$\cos\omega = \sum_{i=1}^{n+1} \xi^i \eta^i = \sum_{i=1}^{n+1} \frac{(z^iU)(z^iV)}{\sqrt{(fU)^2}\sqrt{(fV)^2}} = \frac{(fU)(fV)}{\sqrt{(fU)^2}\sqrt{(fV)^2}}. \tag{16}$$

Thus *a necessary and sufficient condition for orthogonality of the two curves is*

$$(fU)(fV) = 0. \tag{17}$$

Equation (17) also defines the orthogonal trajectories of a system of U-curves on R_n. An illustration is found in the case of curves on an ordinary surface.

§ 3. *Lines of Curvature on R.*

A line L drawn on R_n such that the normals to R_n along L (with respect to the enclosing space S_{n+1}) generate a developable surface is called* a line of curvature of R_n in S_{n+1}.

At a point P of R_n there is a unique normal to R_n in S_{n+1}. Let the direction cosines of this normal be $\zeta', \cdots, \zeta^{n+1}$. Choose P as origin of the system of x-axes on R_n. Then, since the normal to R_n at P is orthogonal to every direction on R_n at P, we have from (7)

$$\sum_{i=1}^{n+1} \zeta^i z_k^i = 0 \qquad (k = 1, \cdots, n). \tag{18}$$

The coefficients a_{ik} of the first fundamental form of R_n, given in (3) are the first fundamental quantities. The second fundamental quantities are defined by the equations

$$a_{ik} = \sum_{j=1}^{n+1} \zeta^j z^j_{ik} \qquad (i, k = 1, \cdots, n).$$

*Cf. BIANCHI, *Lezioni di Geometria Differenziale*, vol. I, p. 125.

By differentiating (18), one obtains

$$\alpha_{ik} = \sum_{j=1}^{n+1} \zeta^j z^j_{ik} = -\sum_{j=1}^{n+1} \zeta^j_i z^j_k \qquad (i, k = 1, \cdots, n). \tag{19}$$

The letters g and γ are to be used in this paper as symbols of the second fundamental quantities

$$\alpha_{ik} = g_i g_k = \gamma_i \gamma_k = \alpha_{ki}. \tag{20}$$

Let C be the curve of S_{n+1} which is the envelope of the normals along L. Let $M(z', \cdots, z^{n+1})$ be any point of L, and $\overline{M}(\overline{z}', \cdots, \overline{z}^{n+1})$ be the point where the normal at M meets C. Denote by r the distance $M\overline{M}$, which is positive or negative according to the direction of $\overline{M}$ from M. Then

$$\overline{z}' = z' - r\zeta', \ \cdots, \ \overline{z}^{n+1} = z^{n+1} - r\zeta^{n+1}. \tag{21}$$

Take derivatives of equations (21) with respect to the arc s of L. Then, since C is envelope of the normals along L,

$$\begin{aligned} \frac{d\overline{z}'}{ds} &= \frac{dz'}{ds} - r\frac{d\zeta'}{ds} - \zeta'\frac{dr}{ds} = q\zeta', \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \frac{d\overline{z}^{n+1}}{ds} &= \frac{dz^{n+1}}{ds} - r\frac{dz^{n+1}}{ds} - \zeta^{n+1}\frac{dr}{ds} = q\zeta^{n+1}, \end{aligned} \tag{22}$$

where q is a factor of proportionality to be determined. Multiply equations (22) by $\zeta', \cdots, \zeta^{n+1}$ in order and add. We get

$$q\sum_{i=1}^{n+1}[\zeta^i]^2 = \sum_{i=1}^{n+1}\zeta^i\frac{dz^i}{ds} - r\sum_{i=1}^{n+1}\zeta^i\frac{d\zeta^i}{ds} - \frac{dr}{ds}\sum_{i=1}^{n+1}[\zeta^i]^2. \tag{23}$$

Now

$$\sum_{i=1}^{n+1}[\zeta^i]^2 = 1, \qquad \sum_{i=1}^{n+1}\zeta^i\frac{d\zeta^i}{ds} = 0, \qquad \sum_{i=1}^{n+1}\zeta^i\frac{dz^i}{ds} = 0,$$

since $\zeta', \cdots, \zeta^{n+1}$ are direction cosines of the normal and $dz'/ds, \cdots, dz^{n+1}/ds$ are direction cosines of L. Substituting these results in (23), one obtains

$$q = -\frac{dr}{ds}.$$

Then equations (22) give

$$\frac{dz'}{ds} = r\frac{d\zeta'}{ds}, \ \cdots, \ \frac{dz^{n+1}}{ds} = r\frac{d\zeta^{n+1}}{ds}, \tag{24}$$

or

$$\frac{dz'}{d\zeta} = \frac{dz^2}{d\zeta^2} = \cdots = \frac{dz^{n+1}}{d\zeta^{n+1}} = r. \tag{25}$$

This result is expressed in curvilinear coördinates as follows:

$$z_1' dx_1 + \cdots + z_n' dx_n = r(\zeta_1' dx_1 + \cdots + \zeta_n' dx_n),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$z_1^{n+1} dx_1 + \cdots + z_n^{n+1} dx_n = r(\zeta_1^{n+1} dx_1 + \cdots + \zeta_n^{n+1} dx_n).$$

Multiply these equations in order by z_k', $\cdots$, z_k^{n+1} and add. We find

$$\sum_{i=1}^{n+1} z_k^i z_1^i dx_1 + \cdots + \sum_{i=1}^{n+1} z_k^i z_n^i dx_n = r\left[\sum_{i=1}^{n+1} z_k^i \zeta_1^i dx_1 + \cdots + \sum_{i=1}^{n+1} z_k^i \zeta_n^i dx_n\right].$$

Then, by (4) and (19),

$$a_{k1} dx_1 + \cdots + a_{kn} dx_n = -r[\alpha_{k1} dx_1 + \cdots + \alpha_{kn} dx_n] \quad (k = 1, \cdots, n). \tag{26}$$

Equations (26) hold for every line of curvature on R_n. Conversely, if equations (26) be true for any curve L on R_n, then there exists a curve C in S_{n+1} whose tangents are normal to R_n along L, so that L is a line of curvature on R_n by definition.

When equations (26) are written in the form

$$\begin{aligned}(a_{11} + \alpha_{11} r) dx_1 + \cdots + (a_{1n} + \alpha_{1n} r) dx_n &= 0,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\

If now a line of curvature be represented as a U-curve (10), one gets from (13) and (29)

$$f_k(fU) = -rg_k(gU) \qquad (k=1, \cdots, n). \tag{30}$$

A symmetrical expression for r is obtained by multiplying equations (30) in order by the cofactors of $f_1, \cdots, f_n$ in (fU) and adding:

$$r = -\frac{(fU)^2}{(gU)^2}. \tag{31}$$

If any two lines of curvature through P be given as U and V-curves, and their respective curvatures be denoted by $1/r'$ and $1/r''$, one gets from (30)

$$g_1(gU) = -\frac{1}{r'}f_1(fU), \ \cdots, \ g_n(gU) = -\frac{1}{r'}f_n(fU),$$

$$g_1(gV) = -\frac{1}{r''}f_1(fV), \ \cdots, \ g_n(gV) = -\frac{1}{r''}f_n(fV).$$

Multiply the equations of the first line in order by the cofactors of $f_1, \cdots, f_n$ in (fV) and add. Also multiply the equations of the second line in order by the cofactors of $f_1, \cdots, f_n$ in (fU) and add. Then

$$(gU)(gV) = -\frac{1}{r'}(fU)(fV) = -\frac{1}{r''}(fU)(fV),$$

so that either $r' = r''$ or $(fU)(fV) = 0$. Hence by (17) we have

Theorem I. *Any two distinct lines of curvature through an ordinary point P of R_n are orthogonal to each other.*

If the lines of curvature through P be taken as parameter lines, then, by (9),

$$a_{ik} = 0 \qquad (i \neq k).$$

It follows at once from (26) that also

$$\alpha_{ik} = 0 \qquad (i, k=1, \cdots, n; i \neq k).$$

Theorem II. *If the lines of curvature at an ordinary (not umbilic) point of R_n be taken as parameter lines, then*

$$a_{ik} = 0, \qquad \alpha_{ik} = 0 \qquad (i, k=1, \cdots, n; i \neq k).$$

§4. *Definition of the Curvatures of R_n in S_{n+1}.*

Equation (28) may be written in the form

$$H_0 + H_1 r + \cdots + H_{n-1}r^{n-1} + H_n r^n = 0, \tag{32}$$

where*

$$H_0 = |a_{ik}| = 1/\beta^2, \qquad H_n = |\alpha_{ik}|,$$

* M. I., (9).

while for $j = 1, \cdots, n$, H_j is the sum of all the determinants obtained from $|a_{ik}|$ by replacing in all possible ways j columns of $|a_{ik}|$ by the corresponding columns of $|\alpha_{ik}|$. Dividing (32) by H_0 one obtains

$$1 + K_1 r + \cdots + K_{n-1} r^{n-1} + K_n r^n = 0. \tag{33}$$

The coefficient K_n (the product of all the curvatures) is the Kronecker-Gaussian curvature of hyperspace. It has been shown to be expressible in terms of the first fundamental quantities and their derivatives (cf. K–G. C.). In this paper the coefficients of (33) are called the n curvatures of R_n in S_{n+1}. By definition

$$K_1 = \beta^2 \sum_{i,k}^{1,\cdots,n} \alpha_{ik} A_k^i, \qquad K_2 = \beta^2 \sum_{i_1 i_2, k_1 k_2}^{1,\cdots,n} \begin{vmatrix} \alpha_{i_1 k_1} & \alpha_{i_1 k_2} \\ \alpha_{i_2 k_1} & \alpha_{i_2 k_2} \end{vmatrix} \cdot A_{k_1 k_2}^{i_1 i_2} = \sum_{i_1 i_2 k_1 k_2}^{1,\cdots,n} \Delta_{\substack{i_1 i_2 \\ k_1 k_2}} A_{k_1 k_2}^{i_1 i_2}, \cdots,$$

$$K_m = \beta^2 \sum_{i_1 \cdots i_m k_1 \cdots k_m}^{1,\cdots,n} \Delta_{\substack{i_1 \cdots i_m \\ k_1 \cdots k_m}} \cdot A_{k_1 \cdots k_m}^{i_1 \cdots i_m} \qquad (m = 1, \cdots, n), \tag{34}$$

where A_k^i is the cofactor of a_{ik} in $|a_{ik}|$, $A_{k_1 k_2}^{i_1 i_2}$ is the *algebraic complement* of

$$\begin{vmatrix} a_{i_1 k_1} a_{i_1 k_2} \\ a_{i_2 k_1} a_{i_2 k_2} \end{vmatrix}$$

in $|a_{ik}|$, while $\Delta_{\substack{i_1 i_2 \\ k_1 k_2}}$ is the *second minor* of $|\alpha_{ik}|$ indicated for K_2 above; and similarly for the A's and Δ's in K_m. Both sets $i_1, \cdots, i_m$ and $k_1, \cdots, k_m$ are considered as being in ascending numerical order.

§ 5. *Invariant Symbolic Forms of* $K_1, \cdots, K_n$.

If F_k^i be the cofactor of f_k^i in the functional determinant $\{f', \cdots, f^n\}$, Maschke * has shown that

$$A_k^i = \frac{1}{(n-1)!} F'_i F'_k.$$

Thus

$$K_1 = \beta^2 \sum_{i,k}^{i,\cdots,n} \alpha_{ik} A_k^i = \frac{\beta^2}{(n-1)!} \sum_{i,k}^{i,\cdots,n} g_i g_k F'_i F'_k$$

$$= \frac{\beta^2}{(n-1)!} \{gf^2 \cdots f^n\}^2 = \frac{1}{(n-1)!} (gf)^2.$$

This suggests a method for reducing all the curvatures to convenient invariant forms. Let $F_{i_1 \cdots i_m}^{1 \cdots m}$ be the algebraic complement of

$$\begin{vmatrix} f'_{i_1} & \cdots & f'_{i_m} \\ \cdots & \cdots & \cdots \\ f_{i_1}^m & \cdots & f_{i_m}^m \end{vmatrix}$$

* M. I., p. 450.

in $\{f' \cdots f^n\}$. Then the product $F^{1\cdots m}_{i_1\cdots i_m} \cdot F^{1\cdots m}_{k_1\cdots k_m}$ may be written

$$\begin{vmatrix} f_1^{m+1} \cdots f_{i_1-1}^{m+1} f_{i_1+1}^{m+1} \cdots f_{i_m-1}^{m+1} f_{i_m+1}^{m+1} \cdots f_{i_n}^{m+1} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ f_1^{n} \cdots f_{i_1-1}^{n} f_{i_1+1}^{n} \cdots f_{i_m-1}^{n} f_{i_m+1}^{n} \cdots f_{i_n}^{n} \end{vmatrix} F^{1\cdots m}_{k_1\cdots k_m}.$$

If the first determinant of this product be expanded, one finds $(n-m)!$ terms of the form

$$(-1)^{\mu} f_1 \cdots f_{i_1-1} f_{i_1+1} \cdots f_{i_m-1} f_{i_m+1} \cdots f_n \cdot F^{1\cdots m}_{k_1\cdots k_m},$$

where the suppressed upper indices of the first factor are understood to be any permutation of the numbers $m+1, \cdots, n$, while μ represents the number of inversions in the permutation. Since the equivalent symbols $f^{m+1}, \cdots, f^n$ may be interchanged in all possible ways without altering the value of the term, let them be so interchanged for each term as to reduce the first factor to $(-1)^{\mu}$ times the principal diagonal term of $F^{1\cdots m}_{i_1\cdots i_m}$. This causes an interchange of rows in the second (determinant) factor $F^{1\cdots m}_{k_1\cdots k_m}$ so that it becomes in each case $(-1)^{\mu}$ times its original form. Hence the above product becomes

$$(n-m)! f_1^{m+1} \cdots f_{i_1-1}^{m+1} f_{i_1+1}^{i_1+m-1} f_{i_1+1}^{i_1+m} \cdots f_{i_m-1}^{i_m} f_{i_m+1}^{i_m+1} \cdots f_n^n \cdot F^{1\cdots m}_{k_1\cdots k_m}.$$

Multiplying each f into the corresponding row of the determinant $F^{1\cdots m}_{k_1\cdots k_m}$ (which has a form similar to that given above for $F^{1\cdots m}_{i_1\cdots i_m}$), we have

$$F^{1\cdots m}_{i_1\cdots i_m} \cdot F^{1\cdots m}_{k_1\cdots k_m} = (n-m)!\, A^{i_1\cdots i_m}_{k_1\cdots k_m},$$

or

$$A^{i_1\cdots i_m}_{k_1\cdots k_m} = \frac{1}{(n-m)!} F^{1\cdots m}_{i_1\cdots i_m} \cdot F^{1\cdots m}_{k_1\cdots k_m}. \tag{35}$$

Also

$$\Delta^{i_1\cdots i_m}_{k_1\cdots k_m} = \begin{vmatrix} \alpha_{i_1k_1} \cdots \alpha_{i_1k_m} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \alpha_{i_mk_1} \cdots \alpha_{i_mk_m} \end{vmatrix} = \begin{vmatrix} g'_{i_1}g'_{k_1} \cdots g'_{i_1}g'_{k_m} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ g^m_{i_m}g^m_{k_1} \cdots g^m_{i_m}g^m_{k_m} \end{vmatrix} = g'_{i_1} \cdots g^m_{i_m} \begin{vmatrix} g'_{k_1} \cdots g'_{k_m} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ g^m_{k_1} \cdots g^m_{k_m} \end{vmatrix},$$

$$\Delta^{i_1\cdots i_m}_{k_1\cdots k_m} = \frac{1}{m!} \begin{vmatrix} g'_{i_1} \cdots g'_{i_m} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ g^m_{i_1} \cdots g^m_{i_m} \end{vmatrix} \cdot \begin{vmatrix} g'_{k_1} \cdots g'_{k_m} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ g^m_{k_1} \cdots g^m_{k_m} \end{vmatrix}. \tag{36}$$

Substituting (35) and (36) in (34), one finds, by a well-known theorem of determinants,

$$K_m = \frac{1}{m!(n-m)!}(g' \cdots g^m f^{m+1} \cdots f^n)^2 = \frac{1}{m!(n-m)!}(g' \cdots g^m f)^2. \tag{37}$$

In particular,

$$K_1 = \frac{1}{(n-1)!}(gf)^2 = \Delta_1 g,$$

where, by M. I. (22), $\Delta_1 g$ is the first differential parameter of the first quadratic form ( ).

Since the other coefficients are corresponding differential parameters (the number of g's being the same as the subscript of K), it would seem fitting to generalize the notation and set *

$$K_m = \frac{1}{m!(n-m)!}(g' \cdots g^m f)^2 = \Delta^m g, \tag{38}$$

with the note that $\Delta' g = \Delta_1 g$.

§ 6. *Expression of $K_{2\nu}$ in terms of the first Fundamental Quantities and Derivatives.*

The generalization of the Gauss equation shows that any second order determinant of the second fundamental quantities is equal to a Riemann quadruple index symbol, which is expressible in terms of the first fundamental quantities and derivatives.† By K.–G. C. (27),

$$\begin{vmatrix} \alpha_{i_1 k_1} \alpha_{i_1 k_2} \\ \alpha_{i_2 k_1} \alpha_{i_2 k_2} \end{vmatrix} = (i_1 i_2 k_1 k_2) = \frac{1}{(n-1)!} f'_{i_1} f^2_{i_2} \begin{vmatrix} (fa)'_{k_1} (fa)'_{k_2} \\ (fa)^2_{k_1} (fa)^2_{k_2} \end{vmatrix}.$$

By an easy induction, any even order determinant of the α's is expressed in terms of the symbols of the a's as follows: ‡

$$\Delta^{i_1 \cdots i_{2\nu}}_{k_1 \cdots k_{2\nu}} = \frac{\epsilon^\nu}{(2\nu)!} \begin{vmatrix} (fa)'_{i_1} \cdots (fa)'_{i_{2\nu}} \\ \cdots\cdots\cdots \\ (fa)^{2\nu}_{i_1} \cdots (fa)^{2\nu}_{i_{2\nu}} \end{vmatrix} \cdot \begin{vmatrix} f'_{k_1} \cdots f'_{k_{2\nu}} \\ \cdots\cdots \\ f^{2\nu}_{k_1} \cdots f^{2\nu}_{k_{2\nu}} \end{vmatrix}, \tag{39}$$

where $\epsilon = 1/(n-1)!$; the symbol $(fa)^j$ contains f^j and $a^2 \cdots a^n$, while the symbols a in every consecutive pair $(fa^2 \cdots a^n)^{2\lambda-1}$, $(fa^2 \cdots a^n)^{2\lambda}$ are equal when they have the same index, otherwise they are distinct but equivalent symbols of the first fundamental form (3).

Now from (34), (35), and (39),

$$K_{2\nu} = \frac{\beta^2 \epsilon^\nu}{(2\nu)!(n-2\nu)!} \sum_{i_1 \cdots i_{2\nu} k_1 \cdots k_{2\nu}}^{1 \cdots n} \begin{vmatrix} (fa)'_{i_1} \cdots (fa)'_{i_{2\nu}} \\ \cdots\cdots\cdots \\ (fa)^{2\nu}_{i_1} \cdots (fa)^{2\nu}_{i_{2\nu}} \end{vmatrix} \cdot \begin{vmatrix} (f'_{k_1} \cdots f'_{k_{2\nu}} \\ \cdots\cdots \\ (f^{2\nu}_{k_1} \cdots f^{2\nu}_{k_{2\nu}} \end{vmatrix} \times F^{1 \cdots 2\nu}_{i_1 \cdots i_{2\nu}} F^{1 \cdots 2\nu}_{k_1 \cdots k_{2\nu}},$$

or

$$K_{2\nu} = \frac{\epsilon^\nu}{(2\nu)!(n-2\nu)!} \big((fa)' \cdots (fa)^{2\nu} f \big)(f). \tag{40}$$

* The use of $\Delta_m g$ would conflict with the second differential parameter of ordinary differential geometry, which has an entirely different meaning. Cf. BIANCHI, *Lezioni di Geometria Differenziale*, vol. I, p. 67.

† M. I., (117)–(126).

‡ Cf. K.–G. C., (28).

This gives Maschke's expression * for K_n when n is even:

$$K_n = \frac{1}{n![(n-1)!]^{n/2}}\big((fa)'\cdots(fa)^{n}\big)(f) \qquad (n \text{ even}).$$

Theorem. *The mean curvatures $K_{2\nu}$, with even subscript, are represented in* (40) *as rational integral functions of the coefficients of the first fundamental form and their derivatives.*

§ 7. *Expression of $K_{2\nu+1}$ in terms of the first Fundamental Quantities and Derivatives, when ν is greater than zero.*

Use is made of the determinant theorem

$$(41)\quad \Delta^2_{\substack{i_1\cdots i_{2\nu+1}\\ k_1\cdots k_{2\nu+1}}} = \frac{1}{2}\sum_{j,r}^{1,\cdots,n}\begin{vmatrix}\alpha_{i_jk_s} & \alpha_{i_jk_t}\\ \alpha_{i_rk_s} & \alpha_{i_rk_t}\end{vmatrix}\cdot\begin{vmatrix}D_{i_jk_s} & D_{i_jk_t}\\ D_{i_rk_s} & D_{i_rk_t}\end{vmatrix} \qquad (s,t=1,\cdots,2\nu+1;\ s\neq t),$$

where $\nu \neq 0$ and the D's are cofactors of the corresponding α's in $\Delta^{i_1\cdots i_{2\nu+1}}_{k_1\cdots k_{2\nu+1}}$ and are therefore all of even order and expressible by (39). The results are

$$D_{i_jk_s} = \frac{\epsilon^\nu}{(2\nu)!}F'_{i_j}(FA)'_{k_s}, \qquad D_{i_jk_t} = \frac{\epsilon^\nu}{(2\nu)!}\Phi'_{i_j}(\Phi B)'_{k_t},$$

$$D_{i_rk_s} = \frac{\epsilon^\nu}{(2\nu)!}F'_{i_r}(FA)'_{k_s}, \qquad D_{i_rk_t} = \frac{\epsilon^\nu}{(2\nu)!}\Phi'_{i_r}(\Phi B)'_{k_t},$$

where F'_{i_j} is the cofactor of f'_{i_j} in $\{f'_{i_1}\cdots f^{2\nu+1}_{i_{2\nu+1}}\}$, $\cdots$, $(\Phi B)'_{k_t}$ is the cofactor of $(\phi b)'_{k_t}$ in $\{(\phi b)'_{k_1}\cdots(\phi b)^{2\nu+1}_{k_{2\nu+1}}\}$. Also, by M. I. (120),

$$\begin{vmatrix}\alpha_{i_jk_s} & \alpha_{i_jk_t}\\ \alpha_{i_rk_s} & \alpha_{i_rk_t}\end{vmatrix} = \epsilon(fc)'_{k_s}(\phi c)'_{k_t}\begin{vmatrix}f'_{i_j} & \phi'_{i_j}\\ f'_{i_r} & \phi'_{i_r}\end{vmatrix},$$

Substituting in (41), we find

$$\Delta^2_{\substack{i_1\cdots i_{2\nu+1}\\ k_1\cdots k_{2\nu+1}}} = \frac{\epsilon^{2\nu+1}}{[(2\nu)!]^2}(fc)'_{k_s}(FA)'_{k_s}(\phi c)'_{k_t}(\Phi B)'_{k_t} \times\frac{1}{2}\sum_{j,r}^{1\cdots 2\nu+1}\begin{vmatrix}f'_{i_j} & \phi'_{i_j}\\ f'_{i_r} & \phi'_{i_r}\end{vmatrix}\cdot\begin{vmatrix}F'_{i_j} & \Phi'_{i_j}\\ F'_{i_r} & \Phi'_{i_r}\end{vmatrix}.$$

This last sum expands into

$$\frac{1}{2}\sum_{j,r}^{1,\cdots,2\nu+1}[f'_{i_j}F'_{i_j}\phi'_{i_r}\Phi'_{i_r} - f'_{i_j}\Phi'_{i_j}\phi'_{i_r}F'_{i_r} - f'_{i_r}\Phi'_{i_r}\phi'_{i_j}F'_{i_j} + f'_{i_r}F'_{i_r}\phi'_{i_j}\Phi'_{i_j}] = \begin{vmatrix}\{f'_{i_1}\cdots f^{2\nu+1}_{i_{2\nu+1}}\} & \{f'_{i_1}\phi^2_{i_2}\cdots\phi^{2\nu+1}_{i_{2\nu+1}}\}\\ \{\phi'_{i_1}f^2_{i_2}\cdots f^{2\nu+1}_{i_{2\nu+1}}\} & \{\phi'_{i_1}\cdots\phi^{2\nu+1}_{i_{2\nu+1}}\}\end{vmatrix},$$

so that

$$\Delta^2_{\substack{i_1\cdots i_{2\nu+1}\\ k_1\cdots k_{2\nu+1}}} = \frac{\epsilon^{2\nu+1}}{[(2\nu)!]^2}(fc)'_{k_s}(FA)'_{k_s}(\phi c)'_{k_t}(\Phi B)'_{k_t} \times\begin{vmatrix}\{f'_{i_1}\cdots f^{2\nu+1}_{i_{2\nu+1}}\} & \{f'_{i_1}\phi^2_{i_2}\cdots\phi^{2\nu+1}_{i_{2\nu+1}}\}\\ \{\phi'_{i_1}f^2_{i_2}\cdots f^{2\nu+1}_{i_{2\nu+1}}\} & \{\phi'_{i_1}\cdots\phi^{2\nu+1}_{i_{2\nu+1}}\}\end{vmatrix}.$$

* K.-G. C., (29).

By (41) this equation holds for all values of s and t from 1 to $2\nu+1$ except $s=t$. When $s=t$, the second member vanishes. Sum the equations given by using all values of s and t from 1 to $2\nu+1$ and divide by $(2\nu+1)2\nu$; also multiply by β^i. Then

$$\beta^i \Delta^2_{\substack{i_1 \cdots i_{2\nu+1} \\ k_1 \cdots k_{2\nu+1}}} = \frac{\varepsilon^{2\nu+1}}{(2\nu+1)(2\nu)[(2\nu)!]^2} \left((fc)'_{k_1} (fa)^2_{k_2} \cdots (fa)^{2\nu+1}_{k_{2\nu+1}} \right)$$

(42)

$$\times \left((\phi c)'_{k_1} (\phi b)^2_{k_2} \cdots (\phi b)^{2\nu+1}_{k_{2\nu+1}} \right) \begin{vmatrix} \{ f'_{i_1} \cdots f^{2\nu+1}_{i_{2\nu+1}} \} & \{ f'_{i_1} \phi^2_{i_2} \cdots \phi^{2\nu+1}_{i_{2\nu+1}} \} \\ \{ \phi'_{i_1} f^2_{i_2} \cdots f^{2\nu+1}_{i_{2\nu+1}} \} & \{ \phi'_{i_1} \cdots \phi^{2\nu+1}_{i_{2\nu+1}} \} \end{vmatrix}.$$

And by (34)

$$K_{2\nu+1} = \sum_{i_1 \cdots i_{2\nu+1} k_1 \cdots k_{2\nu+1}}^{1, \ldots, n} [\beta^i \Delta^2_{\substack{i_1 \cdots i_{2\nu+1} \\ k_1 \cdots k_{2\nu+1}}}]^{\frac{1}{2}} A_{\substack{i_1 \cdots i_{2\nu+1} \\ k_1 \cdots k_{2\nu+1}}} \qquad (\nu > 0).$$

Thus by (34) and (42) we have $K_{2\nu+1} (\nu > 0)$ expressed in terms of the first fundamental quantities and derivatives (but only in the irrational form of a sum of square roots).

The case of K_1 presents special difficulty:

$$K_1 = \beta^2 \sum_{ik}^{1, \ldots, n} \alpha_{ik} A^i_k.$$

In K.–G. C. (p. 24), Maschke suggests a method for expressing the α's in terms of the a's when n is odd. His formula (24) should, however, be written,

$$\alpha_{11} \Delta^{n-2} = \begin{vmatrix} A_{22} \cdots A_{2n} \\ A_{n2} \cdots A_{nn} \end{vmatrix}. \tag{43}$$

If n is odd, the elements of the second member of (43) are of even order, and therefore expressible by (39), and similarly for every α. But Δ itself is of odd order, and is raised to an odd power ($n-2$ instead of $n-1$).* Equation (43) is true also for even values of n, so that the α's are always expressible by (43) in terms of the first fundamental quantities and derivatives (if $n > 2$), but in all cases irrationally.

Using (43), the author has calculated irrational values of K_1 when n is greater than two; but the notation is so complicated that the presentation of the results seems impracticable, if not also useless.†

If $2\nu+1=n$, the sum reduces to a single term and formulas (34) and (42)

*Cf. BÔCHER, *Introduction to Higher Algebra*, § 11.

† In a recent paper the author has calculated the value of K_1 as well as of the other curvatures of odd subscript, for a space of $n-1$ dimensions defined in R_n by the equation $U(x_1 \cdots x_n) = 0$. These values involve only the coefficients of the first fundamental form of R_n and their derivatives, together with the function U.

give a rational value for K_n^2,

$$(44)\quad K_n^2=\beta^1\Delta^2=\frac{\epsilon^{n+2}}{n(n-1)}\big((fc)'(fa)^2\cdots(fa)^n\big)\big((\phi c)'(\phi b)^2\cdots(\phi b)^n\big)\begin{vmatrix}(f) & (f'\phi)\\ (\phi' f) & (\phi)\end{vmatrix}.$$

By the method used in K.–G. C. (p. 86), this may be reduced to Maschke's form (31):*

$$(45)\quad K_n^2=\frac{1}{n[(n-1)!]^{n+2}}\big((fc)'(fa)^2\cdots(fa)^n\big)\big((\phi c)'(\phi b)^2\cdots(\phi b)^n\big)(f'\phi' f)(f^2\phi^2\phi).$$

The rather unsatisfactory results of this section are then as follows:

If n is odd, K_n^2 is expressed by (45) *as a rational function of the first fundamental quantities and their derivatives. Equations* (34) *and* (42) *give irrational expressions for the curvatures of odd index except K_1, for which no expression is here given.*

PART II.

Invariants of R_λ in R_n.

The quantities $K_{2\nu}$ and K_n^2, for n odd, are by their forms (40) and (45) differential invariants of the first fundamental quadratic form (3). When (3) defines the arc-element of a space R_n of n dimensions contained in an euclidean space S_{n+1} of $n+1$ dimensions, these K's have the geometric meaning already assigned to them. It is our object† to find corresponding invariants of a space R_λ of λ dimensions, represented as differential parameters of a general space R_n of higher dimensions containing R_λ.

§ 1. *Definitions and Preliminary Formulas.*

In the general space R_n, of n dimensions, whose coördinates are $x_1, \cdots, x_n$ and whose arc-element is defined by equation (3), let the space R_λ of λ dimensions ($\lambda < n$) be defined by the $n-\lambda$ equations

$$(46)\qquad U^{\lambda+1}(x_1, \cdots, x_n)=\text{const.}, \cdots, U^n(x_1, \cdots, x_n)=\text{const.}$$

If λ other arbitrarily chosen functions of $x_1, \cdots, x_n$, say $u', \cdots, u^\lambda$, such that

$$\Delta=(u'\cdots u^\lambda U^{\lambda+1}\cdots U^n)\neq 0,$$

are adjoined to these, the space R_λ may also be represented in parametric form

$$(47)\qquad x_1=x_1(u', \cdots, u^\lambda), \cdots, x_n=x_n(u', \cdots, u^\lambda),$$

* In Maschke's reduction there are two slight numerical errors which balance each other. His equation (30) differs from (44) above in that he has divided by n^2 instead of by $n(n-1)$; while in his reduction of (30) there are $n-1$ of the terms which become equal, instead of n.

† Cf. K.–G. C., § 5.

by solving the $n - \lambda$ equations (46) with the λ equations

$$u'(x_1, \cdots, x_n) = u', \cdots, u^\lambda(x_1, \cdots, x_n) = u^\lambda. \tag{48}$$

Any n differentials satisfying the $n - \lambda$ equations, found by differentiating (46),

$$\sum_{i=1}^{n} U_i^{\lambda+1} dx_i = 0, \cdots, \quad \sum_{i=1}^{n} U_i^n dx_i = 0$$

determine a certain direction in R_λ. In order to find these differentials in terms of $du', \cdots, du^\lambda$, we differentiate also equations (48) and solve the set

$$\begin{aligned}
u_1' dx_1 + \cdots + u_n' dx_n &= du', \\
&\cdots \\
u_1^\lambda dx_1 + \cdots + u_n^\lambda dx_n &= du^\lambda, \\
U_1^{\lambda+1} dx_1 + \cdots + U_n^{\lambda+1} dx_n &= 0, \\
&\cdots \\
U_1^n dx_1 + \cdots + U_n^n dx_n &= 0.
\end{aligned}$$

If A^{kr} be the cofactor of u_r^k in Δ, then

$$dx_r = \frac{1}{\Delta} \sum_{k=1}^{\lambda} A^{kr} du^k$$

and therefore,

$$\sum_{r=1}^{n} p_r dx_r = \frac{1}{\Delta} \sum_{k=1}^{\lambda} \{u' \cdots u^{k-1} p u^{k+1} \cdots u^\lambda U\} du^k, \tag{49}$$

where p is any ordinary function of $x_1, \cdots, x_n$.

In order to find the expression for ds in terms of $u', \cdots, u^\lambda$, we introduce for the differential quantic (3) the symbolic form

$$ds^2 = \sum_{i,k}^{1,\cdots,n} a_{ik} dx_i dx_k = \left[\sum_{i=1}^{n} f_i dx_i \right]^2.$$

Then (49) gives for the length element in R_λ

$$\begin{aligned}
ds^2 &= \frac{1}{\Delta^2} \left[\sum_{i=1}^{\lambda} \{u' \cdots u^{i-1} f u^{i+1} \cdots u^\lambda U\} du_i \right]^2 \\
&= \frac{1}{\beta^2 \Delta^2} \left[\sum_{i=1}^{\lambda} (u' \cdots u^{i-1} f u^{i+1} \cdots u^\lambda U) du_i \right]^2.
\end{aligned} \tag{50}$$

We may also introduce for ds^2, as given in terms of $u', \cdots, u^\lambda$, the symbolic form

$$ds^2 = \left[\sum_{i=1}^{\lambda} \mathfrak{f}_i du^i \right]^2. \tag{51}$$

By comparing (50) and (51) we find

$$\mathfrak{f}_i = \frac{1}{\Delta} \{u' \cdots u^{i-1} f u^{i+1} \cdots u^\lambda U\} = \frac{1}{\beta \Delta} (u' \cdots u^{i-1} f u^{i+1} \cdots u^\lambda U). \tag{52}$$

If we use the symbols of form (51), the invariants $K_{2\nu}$ and K^2_λ (λ odd) of R_λ may be written, by (40) and (45),

$$(53)\quad (2\nu)!\,(\lambda-2\nu)!\,[(\lambda-1)!]^\nu K_{2\nu} = G_{2\nu} = \big((\mathfrak{f}\mathfrak{a})'\cdots(\mathfrak{f}\mathfrak{a})^{2\nu}\mathfrak{f}^{2\nu+1}\cdots\mathfrak{f}^\lambda\big)(\mathfrak{f}'\cdots\mathfrak{f}^\lambda),$$

$$(54)\quad \begin{aligned}\lambda\,[(\lambda-1)!]^{\lambda+2} K^2_\lambda = G^2_\lambda = &\big((\mathfrak{f}\mathfrak{c})'(\mathfrak{f}\mathfrak{a})^2\cdots(\mathfrak{f}\mathfrak{a})^\lambda\big)\\ &\times\big((\mathfrak{g}\mathfrak{c})'(\mathfrak{g}\mathfrak{b})^2\cdots(\mathfrak{g}\mathfrak{b})^\lambda\big)(\mathfrak{f}'\mathfrak{g}'\mathfrak{f}^3\cdots\mathfrak{f}^\lambda)(\mathfrak{f}^2\mathfrak{g}^2\cdots\mathfrak{g}^\lambda),\end{aligned}$$

where $G_{2\nu}$ and G^2_λ are introduced merely for convenience. In all invariantive brackets containing the new symbols, of the quadratic form (51), the differentiation is with respect to the λ variables u', $\cdots$, u^λ. This is indicated sufficiently by the German type and the number of symbols inside the brackets. β_u is defined by the equation

$$(\mathfrak{f}'\cdots\mathfrak{f}^\lambda) = \beta_u\{\mathfrak{f}'\cdots\mathfrak{f}^\lambda\}.$$

We now proceed to compute the values of the invariantive expressions used in (53) and (54) in terms of the symbols of the first fundamental form (3), of R_n and the functions $U^{\lambda+1}$, $\cdots$, U^n which define R_λ in R_n.

By means of (52) and D. P. (3), we obtain

$$\{\mathfrak{f}'\cdots\mathfrak{f}^\lambda\} = \frac{1}{\Delta^\lambda}\{f'\cdots f^\lambda U\}\{u'\cdots u^\lambda U\}^{\lambda-1} = \frac{1}{\Delta}\{f'\cdots f^\lambda U\},$$

so that

$$(55)\qquad \frac{1}{\beta_u}(\mathfrak{f}'\cdots\mathfrak{f}^\lambda) = \frac{1}{\beta\Delta}(f'\cdots f^\lambda U).$$

To calculate the value of β_u, square (55) and simplify the result by placing $(\mathfrak{f}'\cdots\mathfrak{f}^\lambda)^2 = \lambda!$, according to M. I. (17), and $(f'\cdots f^\lambda U)^2 = \lambda!\,(n-\lambda)!\,\Delta^{n-\lambda}U$ by (38). This gives

$$(56)\qquad \beta_u = \omega\beta\Delta, \qquad \omega = \sqrt{\frac{1}{(n-\lambda)!\,\Delta^{n-\lambda}U}}.$$

Then

$$(\mathfrak{f}'\cdots\mathfrak{f}^\lambda) = \omega(f'\cdots f^\lambda U).$$

The other invariantive forms in (53) and (54) are reduced by the same method, and by interchanging equivalent symbols, giving*

$$(57)\quad \begin{aligned}&(\mathfrak{f}'\mathfrak{g}'\mathfrak{f}^3\cdots\mathfrak{f}^\lambda) = \omega(f'\phi' f^3\cdots f^\lambda U), \qquad (\mathfrak{f}^2\mathfrak{g}^2\cdots\mathfrak{g}^\lambda) = \omega(f'^2\phi^2\cdots\phi^\lambda U)\\ &\big((\mathfrak{f}\mathfrak{a})'\cdots(\mathfrak{f}\mathfrak{a})^{2\nu}\mathfrak{f}^{2\nu+1}\cdots\mathfrak{f}^\lambda\big)\\ &\qquad = \omega\big(\omega(faU)', \omega(faU)^2, \cdots, \omega(faU)^{2\nu}, f^{2\nu+1}\cdots f^\lambda U\big),\end{aligned}$$

* Inside the invariantive brackets, we have followed MASCHKE's custom of omitting commas between symbols, except where ambiguity might occur. Cf. M. I., p. 448.

$$(57)\qquad \begin{aligned}((\mathfrak{fc})'(\mathfrak{fa})^2\cdots(\mathfrak{fa})^\lambda) &= \omega\big(\omega(fcU)', \omega(faU)^2, \cdots, \omega(faU)^\lambda U\big),\\ ((\mathfrak{gc})'(\mathfrak{gb})^2\cdots(\mathfrak{gb})^\lambda) &= \omega\big(\omega(\phi cU)', \omega(\phi bU)^2, \cdots, \omega(\phi bU)^\lambda U\big).\end{aligned}$$

§ 2. *Expression for* $K_{2\nu}$.

By (53) and (57),

$$G_{2\nu} = \omega^2(\omega(faU)', \cdots, \omega(faU)^{2\nu}, f^{2\nu+1}\cdots f^\lambda U)(f'\cdots f^\lambda U).$$

Applying D. P. (4) to the second member, we get

$$G_{2\nu}=\omega^{2\nu+2}\big((faU)'\cdots(faU)^{2\nu}f^{2\nu+1}\cdots f^\lambda U\big)(f'\cdots f^\lambda U)+\omega^{2\nu+1}(f''\cdots f^\lambda U)$$
$$\times\sum_{k=1}^{2\nu}(faU)^k\big((faU)'\cdots(faU)^{k-1}, \omega, (faU)^{k+1}\cdots(faU)^{2\nu}f^{2\nu+1}\cdots f^\lambda U\big).$$

It will now be shown that each term of this last sum vanishes. Aside from the factor $\omega^{2\nu+1}$, each odd term of this sum may be written in the form

$$T=(-1)^{\lambda-1}(f^{k+1}\cdots f^\lambda f'\cdots f^k U)(faU)^k$$
$$\times\big((faU)'\cdots(faU)^{k-1}, \omega, (faU)^{k+1}\cdots(faU)^{2\nu}f^{2\nu+1}\cdots f^\lambda U\big).$$

Applying D. P. (1) to the first two brackets of the second member, we obtain

$$T=(-1)^{\lambda-1}\begin{bmatrix}(f^k f^{k+2}\cdots f^\lambda f'\cdots f^k U)(f^{k+1}a^2\cdots a^\lambda U)\\ +(a^2 f^{k+2}\cdots f^\lambda f''\cdots f^k U)(f^k f^{k+1}a^3\cdots a^\lambda U)\\ +(a^3 f^{k+2}\cdots f^\lambda f'\cdots f^k U)(f^k a^2 f^{k+1}a^4\cdots a^\lambda U)\\ +\quad\cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots\\ +(a^\lambda f^{k+2}\cdots f^\lambda f'\cdots f^k U)(f^k a^2\cdots a^{\lambda-1}f^{k+1}U)\end{bmatrix}$$
$$\times\big((faU)'\cdots(faU)^{k-1}, \omega, (faU)^{k+1}\cdots(faU)^{2\nu}f^{2\nu+1}\cdots f^\lambda U\big).$$

Of these λ terms, the first vanishes because of two identical rows in the first bracket, while the others become equal to each other if we interchange f^{k+1} with $a^2\cdots a^\lambda$ in turn and in each case restore the original order in $(faU)^{k+1}$ by the interchange of two rows.* Thus

$$T=(-1)^{\lambda-1}(1-\lambda)(f^{k+1}\cdots f^\lambda f'\cdots f^k U)(f^k a^2\cdots a^\lambda U)$$
$$\times\big((faU)'\cdots(faU)^{k-1}, \omega, (faU)^{k+1}\cdots\big)=(-1)^{\lambda-1}(1-\lambda)\,T.$$

Hence $T=0$ for odd values of k.

If k is even, each term T may be written

$$T=(f^{k-1}\cdots f^\lambda f'\cdots f^{k-2}U)(faU)^k$$
$$\times\big((faU)'\cdots(faU)^{k-1}, \omega, (faU)^{k+1}\cdots(faU)^{2\nu}f^{2\nu+1}\cdots f^\lambda U\big).$$

*Cf. K.-G. C., p. 92.

By applying D. P. (1) to the first two brackets, and proceeding as above, one finds $T = 0$ also for even values of k.

With the help of these results (58) becomes

$$G_{2\nu} = \omega^{2\nu+2}\big((faU)'\cdots(faU)^{2\nu}f^{2\nu+1}\cdots f^{\lambda}U\big)(f'\cdots f^{\lambda}U).$$

Then, by (53) and (56),

$$(59)\quad K_{2\nu} = \frac{(\lambda-1)!\big((faU)'\cdots(faU)^{2\nu}f^{2\nu+1}\cdots f^{\lambda}U\big)(f'\cdots f^{\lambda}U)}{(2\nu)!(\lambda-2\nu)!\big[(\lambda-1)!(n-\lambda)!\Delta^{n-\lambda}U\big]^{\nu+1}}.$$

If $2\nu = \lambda$, (59) becomes

$$(60)\qquad K_{\lambda} = \frac{\big((faU)'\cdots(faU)^{\lambda}U\big)(f'\cdots f^{\lambda}U)}{\lambda\big[(\lambda-1)!(n-\lambda)!\Delta^{n-\lambda}U\big]^{(\lambda+2)/2}},$$

which agrees with Maschke's form, K.–G. C. (60). The symbols f and a belong to the quadratic form (3), expressing the length element of R_n. Further, $(faU)^s = (f^i a^2\cdots a^{\lambda}U^{\lambda+1}\cdots U^n)$, in which f^i is equal to f^s in $(f'\cdots f^{\lambda}U)$, while the sets of symbols $a^2\cdots a^{\lambda}$ are equal in any two consecutive brackets $(faU)^{2k-1}$, $(faU)^{2k}$ and otherwise distinct.

The result is then that $K_{2\nu}$, for the space R_{λ}, is expressible rationally in terms of the coefficients of the first fundamental form of R_n and their derivatives, together with the functions $U^{\lambda+1}, \ldots, U^n$ (which define R_{λ} in R_n) and their derivatives.

§ 3. *Expression for K_{λ}^2 when λ is odd.**

The invariant K_{λ}^2(λ odd) can be expressed in a manner similar to the above. Substituting from (57) into (54), one gets

$$(61)\quad \begin{aligned} G_{\lambda}^2 &= \omega^4\big(\omega(fcU)', \omega(faU)^2, \ldots, \omega(faU)^{\lambda}U\big)\\ &\quad\times\big(\omega(\phi cU)', \omega(\phi bU)^2, \ldots, \omega(\phi bU)^{\lambda}U\big)\big(f'\phi' f^3\cdots f^{\lambda}U)(f^2\phi^2\cdots\phi^{\lambda}U\big). \end{aligned}$$

By D. P. (4),

$$\begin{aligned} \big(\omega(fcU)', \omega(faU)^2, \ldots, \omega(faU)^{\lambda}U\big) &= \omega^{\lambda}\big((fcU)'(faU)^2\cdots(faU)^{\lambda}U\big)\\ &\quad+\omega^{\lambda-1}(fcU)'\big(\omega, (faU)^2\cdots(faU)^{\lambda}U\big)\\ &\quad+\omega^{\lambda-1}\sum_{i=2}^{\lambda}(faU)^i\big((fcU)'(faU)^2\cdots(faU)^{i-1}, \omega, (faU)^{i+1}\cdots(faU)^{\lambda}U\big)\\ &\equiv \omega^{\lambda}\alpha_1 + \omega^{\lambda-1}\alpha_2 + \omega^{\lambda-1}\alpha_3. \end{aligned}$$

$$\begin{aligned} \big(\omega(\phi cU)', \omega(\phi bU)^2, \ldots, \omega(\phi bU)^{\lambda}U\big) &= \omega^{\lambda}\big((\phi cU)'(\phi bU)^2\cdots(\phi bU)^{\lambda}U\big)\\ &\quad+\omega^{\lambda-1}(\phi cU)'\big(\omega, (\phi bU)^2\cdots(\phi bU)^{\lambda}U\big)\\ &\quad+\omega^{\lambda-1}\sum_{k=2}^{\lambda}(\phi bU)^k\big((\phi cU)'(\phi bU)^2\cdots(\phi bU)^{k-1}, \omega, (\phi bU)^{k+1}\cdots(\phi bU)^{\lambda}U\big)\\ &\equiv \omega^{\lambda}\beta_1 + \omega^{\lambda-1}\beta_2 + \omega^{\lambda-1}\beta_3. \end{aligned}$$

* See K.–G. C., p. 93.

The notations $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3$ are used for brevity to represent the expressions whose relative places they occupy. If we also use

$$\gamma = (f'\phi' f^3 \cdots f^\lambda U), \qquad \delta = (f^2\phi^2 \cdots \phi^\lambda U),$$

then

$$G_\lambda^2 = \omega^{2\lambda+2}[\omega\alpha_1 + \alpha_2 + \alpha_3][\omega\beta_1 + \beta_2 + \beta_3]\gamma\delta. \tag{62}$$

The nine terms of this product (omitting powers of ω) will now be considered in the following order:

1) $\alpha_1\beta_1\gamma\delta$, 4) $\alpha_3\beta_2\gamma\delta$, 7) $\alpha_1\beta_3\gamma\delta$,

2) $\alpha_1\beta_2\gamma\delta$, 5) $\alpha_2\beta_1\gamma\delta$, 8) $\alpha_3\beta_3\gamma\delta$,

3) $\alpha_2\beta_2\gamma\delta$, 6) $\alpha_2\beta_3\gamma\delta$, 9) $\alpha_3\beta_1\gamma\delta$.

For the first we have $\alpha_1\beta_1\gamma\delta = L$, where

$$\begin{aligned} L = &\big((fcU)'(faU)^2 \cdots (faU)^\lambda U\big) \\ &\times \big((\phi cU)'(\phi bU)^2 \cdots (\phi bU)^\lambda U\big)(f'\phi' f^3 \cdots f^\lambda U)(f^2\phi^2 \cdots \phi^\lambda U). \end{aligned} \tag{63}$$

The second is shown to vanish as follows:

$$\begin{aligned} 2)\ \alpha_1\beta_2\gamma\delta &= (f'\phi' f^3 \cdots f^\lambda U)(\phi' c^2 \cdots c^\lambda U) \\ &\quad \times \big((fcU)'(faU)^2 \cdots (faU)^\lambda U\big)(f^2\phi^2 \cdots \phi^\lambda U)\big(\omega, (\phi bU)^2 \cdots (\phi bU)^\lambda U\big) \\ &= \begin{bmatrix} (\phi'\phi' f^3 \cdots f^\lambda U)(f' c^2 \cdots c^\lambda U) \\ +(c^2\phi' f^3 \cdots f^\lambda U)(\phi' f' c^3 \cdots c^\lambda U) \\ +(c^3\phi' f^3 \cdots f^\lambda U)(\phi' c^2 f' c^4 \cdots c^\lambda U) \\ + \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ +(c^\lambda\phi' f^3 \cdots f^\lambda U)(\phi' c^2 \cdots c^{\lambda-1} f' U) \end{bmatrix} \big((fcU)'(faU)^2 \cdots (faU)^\lambda U\big) \cdots \qquad \text{[by D. P. (1)]} \\ &= (1-\lambda)(f'\phi' f^3 \cdots f^\lambda U)(\phi' c^2 \cdots c^\lambda U)\big((fcU)'(faU)^2 \cdots (faU)^\lambda U\big) \cdots \\ &= (1-\lambda)\alpha_1\beta_2\gamma\delta. \end{aligned}$$

Hence the second vanishes. The third and fourth are shown to vanish by applying D. P. (1) to exactly the same expressions.

For the fifth term,

$$\begin{aligned} 5)\ \alpha_2\beta_1\gamma\delta &= (f''\phi' f^3 \cdots f^\lambda U)(f' c^2 \cdots c^\lambda U)\big((\phi cU)'(\phi bU)^2 \cdots (\phi bU)^\lambda U\big) \\ &\quad \times \big(\omega, (faU)^2 \cdots (faU)^\lambda U\big)(f^2\phi^2 \cdots \phi\ U) \\ &= (\phi' f^3 \cdots f^\lambda f' U)(f' c^2 \cdots c^\lambda U)\big((\phi cU)'(\phi bU)^2 \cdots (\phi bU)^\lambda U\big) \cdots . \end{aligned}$$

By applying D. P. (1) to the first two forms and simplifying as for 2), we find

$$\alpha_2\beta_1\gamma\delta = (1-\lambda)\alpha_2\beta_1\gamma\delta.$$

Hence 5) vanishes, and the sixth term is shown to vanish by applying D. P. (1) to the same forms.

For the seventh term,

$$7)\quad \alpha_1\beta_3\gamma\delta = \sum_{k=2}^{\lambda} (\phi^k b^2 \cdots b^\lambda U)(f^2\phi^2 \cdots \phi^\lambda U) \times \big((\phi c U)'(\phi b U)^2 \cdots (\phi b U)^{k-1}, \omega, \cdots\big) \times (f'\phi' f^3 \cdots f^\lambda U)\big((f c U)'(f a U)^2 \cdots (f a U)^\lambda U\big).$$

This sum is shown to vanish for all values of k by the method used for (58), and the vanishing of 8) follows by the same method.

For the last term,

$$9)\quad \alpha_3\beta_1\gamma\delta = \sum_{i=2}^{\lambda} (f a U)^i (f'\phi' f^3 \cdots f^\lambda U) \times \big((f c U)'(f a U)^2 \cdots (f a U)^{i-1}, \omega, (f a U)^{i+1} \cdots (f a U)^\lambda U\big) \times (f^2\phi^2 \cdots \phi^\lambda U)\big((\phi c U)'(\phi b U)^2 \cdots (\phi b U)^\lambda U\big).$$

The terms in which $i > 3$ vanish by the methods used for (58), but the terms T_2 (for $i = 2$) and T_3 (for $i = 3$) do not vanish and require special treatment.

We have $T_2 = (f^3 \cdots f^\lambda f'\phi' U)(f^2 a^2 \cdots a^\lambda U)N$, where

$$N = \big((f c U)', \omega, (f a U)^3 \cdots (f a U)^\lambda U\big)(f^2\phi^2 \cdots \phi^\lambda U) \times \big((\phi c U)'(\phi b U)^2 \cdots (\phi b U)^\lambda U\big),$$

$$T_2 = \begin{bmatrix} (f^2 f^4 \cdots f^\lambda f'\phi' U)(f^3 a^2 \cdots a^\lambda U) \\ +(a_2 f^4 \cdots f^\lambda f'\phi' U)(f^2 f^3 a^3 \cdots a^\lambda U) \\ +(a^3 f^4 \cdots f^\lambda f'\phi' U)(f^2 a^2 f^3 a^4 \cdots a^\lambda U) \\ + \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ +(a^\lambda f^4 \cdots f^\lambda f'\phi' U)(f^2 a^2 \cdots a^{\lambda-1} f^3 U) \end{bmatrix} N \qquad \text{[by D. P. (1)]}$$

$$= (f^2 f^4 \cdots f^\lambda f'\phi' U)(f^3 a^2 \cdots a^\lambda U)N + (1-\lambda)T_2.$$

Hence

$$T_2 = \frac{1}{\lambda}(f^2 f^4 \cdots f^\lambda f'\phi' U)(f^3 a^2 \cdots a^\lambda U)N.$$

If now, we interchange f^2 and f^3 and then restore the regular order of symbols, we get

$$T_2 = -\frac{1}{\lambda}(f'\phi' f^3 \cdots f^\lambda U)(f a U)^2\big((f c U)', (f a U)^2, \omega, (f a U)^4 \cdots (f a U)^\lambda U\big) \times (f^3\phi^2 \cdots \phi^\lambda U)\big((\phi c U)'(\phi b U)^2 \cdots (\phi b U)^\lambda U\big).$$

Next, T_3 may be written as $(f^2\phi^2 \cdots \phi^\lambda U)(f^3 a^2 \cdots a^\lambda U) \cdot P$, where

$$P = \big((fcU)'(faU)^2, \omega, (faU)^4 \cdots (faU)^\lambda U\big) \times (f'\phi' f^3 \cdots f^\lambda U)\big((\phi cU)'(\phi bU)^2 \cdots (\phi bU)^\lambda U\big)\cdot$$

$$T_3 = \begin{bmatrix} (f^3\phi^2 \cdots \phi^\lambda U)(f^2 a^2 \cdots a^\lambda U) \\ +(a^2\phi^2 \cdots \phi^\lambda U)(f^3 f^2 a^3 \cdots a^\lambda U) \\ +(a^3\phi^2 \cdots \phi^\lambda U)(f^3 a^2 f^2 a^4 \cdots a^\lambda U) \\ + \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ +(a^\lambda \phi^2 \cdots \phi^\lambda U)(f^3 a^2 \cdots a^{\lambda-1} f^2 U) \end{bmatrix} P \qquad \text{[by D. P. (1)]}$$

$$= (f^3\phi^2 \cdots \phi^\lambda U)(f^2 a^2 \cdots a^\lambda U)\, P + (1-\lambda)\, T_3,$$

so that $T_3 = -T_2$.

Thus all nine terms in the second member of (62) vanish except the first, whence

$$G_\lambda^2 = \omega^{2\lambda+4} L. \tag{64}$$

Then, by (54) and (56),

$$K_\lambda^2 = \frac{L}{\lambda\,[(\lambda-1)!(n-\lambda)!\Delta^{n-\lambda}U]^{\lambda+2}}, \tag{65}$$

where L is given by (63), in which the symbols f, ϕ, a, b, c belong to the quadratic form (3); the form $(faU)^k = (f^k a^2 \cdots a^\lambda U^{\lambda+1} \cdots U^n)$; the f's (also ϕ's and c's) with same index are equal; the sets of symbols $a^2, \cdots, a^\lambda$ (also $b^2, \cdots, b^\lambda$) are equal in any two consecutive brackets of which the first has even index, and otherwise distinct.

Hence K_λ^2 (λ odd), for the space R_λ, is expressible rationally in terms of the coefficients of the first fundamental form and their derivatives, together with the functions $U^{\lambda+1}, \cdots, U^n$ (which define R_λ in R_n) and their derivatives.

ON THE ORDER OF LINEAR HOMOGENEOUS GROUPS*

(FOURTH PAPER)

BY

H. F. BLICHFELDT

1. In the writer's theorems† on finite groups of linear homogeneous substitutions of determinant unity, a group of special nature called *a self-conjugate* (or *invariant*) *subgroup* H plays an important rôle. There is a lack of completeness to these theorems due to the fact it has not been proved that H is actually less than the transitive (irreducible) group G in which, under certain conditions, it is contained; i. e., the groups G and H may be identical so far as the theorems are concerned. Account had to be taken of this fact in constructing the collineation-groups for the plane and space.‡

The relation between G and H is as follows. Let the number of variables be n, and let V be any substitution of G. The sum of the multipliers of V (weight, characteristic) we shall indicate by (V), which, therefore, represents the sum of n roots of unity:

$$(V) = \sum_{i=1}^{n} \alpha_i \beta_i .$$

Each of these roots we write as the product of one α_i, whose index is prime to a given prime number p, and one β_i, whose index is a power of p. By $(V)_p$ we indicate the quantity obtained by replacing in (V) every root β_i by unity:

$$(V)_p = \sum_{i=1}^{n} \alpha_i .$$

Then, under certain conditions, as mentioned above, there is in G a self-conjugate subgroup H whose substitutions T have the property

$$(VT)_p \equiv (V)_p \pmod{p};$$

from which, in particular,

$$(T)_p \equiv n \pmod{p}.$$

---

* Presented to the Society (San Francisco), September 24, 1910.

† The theorems chiefly concerned are as follows: Theorems 10 and 11 of the article *On the Order of Linear Homogeneous Groups* (*Second Paper*), these **Transactions**, vol. 5 (1904), pp. 315, 317; Theorem 14 of the article *On the Order of Linear Homogeneous Groups* (*Supplement*), *ibid.*, vol. 7 (1906), p. 523. These two articles will be referred to by *LGII* and *LGS* respectively.

‡ **Mathematische Annalen**, vol. 60 (1905), p. 214, § 16; vol. 63 (1907), p. 563, § 15.

2. The writer has recently been able to prove that H (or more strictly, a modified form of it) is actually less than G when this group is primitive, so that in all such cases G cannot be a simple group. Furthermore, it follows that

$$n \equiv 0 \pmod{p}.$$

Theorem 14 of LGS may be modified to read:

THEOREM 14′. *If for $n>1$ a primitive group G in n variables has an abelian subgroup K of order $p^a \geqq p^n$, then G will have an invariant subgroup H which contains at least p^{a-n+1} substitutions of K, but which does not contain K entirely. If T be any substitution of H, and V any substitution of G whose weight (V) is zero,* then*

$$(VT)_p \equiv 0 \pmod{p}.$$

Moreover,

$$(T)_p \equiv 0, \quad \text{and} \quad n \equiv 0 \pmod{p}.$$

Let the substitutions of K be represented by $S_0 = \text{identity}, S_1, \cdots, S_{p^a-1}$.

In proving Theorem 14, LGS, it was first proved that for at least p^{a-n+1} substitutions of K,† say

(1) $$S_0, S_1, \cdots, S_i, \cdots,$$

we have equations of the form

$$(VS_i) - (V) + (1-\theta)X_i = 0,$$

V being any substitution of G, θ a root of the equation

$$\theta^{p^a} - 1 = 0,$$

and X_i a sum of the weights

(2) $$(VS_j) \qquad (j = 0, 1, \cdots, p^a - 1),$$

multiplied by integral functions of θ, the numerical coefficients entering being integers or fractions whose denominators are prime to p.

Now let V be any substitution of G such that (V) is zero. Then

(3) $$(VS_i) + (1-\theta)X_i = 0$$

for all substitutions S_i of the series (1).

Consider all the weights (2).

* BURNSIDE has proved the following theorem: "In any irreducible group of linear substitutions of finite order, other than a cyclical group in a single variable, at least one of its characteristics is zero," Proceedings of the London Mathematical Society, ser. 2, vol. 1 (1903), p. 115.

† Attention is here called to an omission in LGS, page 524. First line below the matrix reads, "Now, to this matrix may be added p^{a-m+1} rows $\cdots$." This should read: "Now, to this matrix may be added $p^{a-m+1}-1$ rows $\cdots$."

First, they may all vanish, whatever be the substitution V chosen, so long as (V) vanishes. By the arguments of § 7, $LGII$, all the substitutions of K and all further substitutions T of G for which (VT) vanishes, form a group H, self-conjugate in G. If H had any weight (W) which vanished, then every (WT) would vanish, and therefore every (T). But this is impossible, since $(S_0) = n$. Accordingly, every weight of H is non-vanishing, and therefore H is intransitive, by Burnside's Theorem. It follows by Theorem 8, $LGII$, and by Burnside's Theorem that H is composed of similarity-substitutions.

Second, the weights (2) do not all vanish. By (3), some of them are divisible by $1-\theta$, the quotient being expressible as a linear function of a finite number of roots of unity, no numerical coefficient entering having a denominator which is divisible by p. Assume that all the weights (2) are divisible by $(1-\theta)^k$, whenever V represents a substitution of G whose weight is divisible by $(1-\theta)^k$, k ranging through the values $0, 1, 2, \cdots, m$; but that the weights (2) are not all divisible by $(1-\theta)^{m+1}$ whenever (V) is divisible by $(1-\theta)^{m+1}$. In general, we should not expect m to be greater than zero. Now, all the substitutions T of G for which

$$(VT) = (1-\theta)^{m+1}X,$$

whenever

$$(V) = (1-\theta)^{m+1}Y,$$

form an invariant subgroup H. To H belongs the series (1), but not the entire group K.

Since G is assumed to be primitive, H, if not composed of similarity-substitutions, must contain a substitution W whose weight vanishes (Theorem 8, $LGII$, and Burnside's Theorem). Then

$$(WT) = (1-\theta)^{m+1}Z$$

for every substitution T of H; i. e., every

$$(WT)_p \equiv 0 \pmod{p},$$

and therefore every

$$(T)_p \equiv 0 \pmod{p}.$$

The Theorems 10 and 11, $LGII$, may be modified in like manner to read that the self-conjugate subgroup H is less than G, the latter being primitive. In addition,

$$(T)_p \equiv 0 \pmod{p}$$

for every substitution of H.

3. One of the most important problems in the theory of linear homogeneous groups is the determination of the maximum order; i. e., the fixing of a superior limit to λ in Jordan's Theorem, the number of variables being given. The

limit known * can now be greatly reduced in special cases. Let G be a primitive group, n the number of variables, and p a prime. Then, using Theorem 14′ in conjunction with Theorem 9, $LGII$, we can prove the

COROLLARY. *If p and n are prime to each other, the highest power of p which divides the order of G must divide $n!\ p^{n-1}$.*

If $n = p$, an invariant subgroup H (assumed to contain and to be greater than the group of similarity-substitutions of order p) must be of order p^k and cannot be abelian, G being assumed primitive. Writing H in monomial form we readily find that, if $k > 3$, it possesses one, and only one, invariant of degree p which can be factored into p linear factors. In such a case G cannot be primitive. Hence, H is of order p^3 (or p^2 when considered as a collineation-group), being generated by the substitutions

$$A\colon\ x_1' = x_1,\ x_2' = \theta x_2,\ \cdots,\ x_p' = \theta^{p-1} a_p;\ \frac{\theta^p - 1}{\theta - 1} = 0;$$

$$B\colon\ x_1' = x_2,\ x_2' = x_3,\ \cdots,\ x_p' = x_1.$$

The order of G is a factor of $(p^2 - 1)p \cdot p^2$ when considered as a collineation-group. The corollary above is therefore true also when $n = p > 2$.

THEOREM 17. *Let G be a primitive collineation-group in n variables, n being a prime > 1. Then the order of G is a factor of*

$$n!\ (2 \cdot 3 \cdot \cdots \cdot p \cdot \cdots)^{n-1}, \tag{4}$$

$2, 3, \cdots, p, \cdots$ being the different primes not greater than the greater of the numbers $4n - 3$, $(n - 2)(2n + 1)$.† The only exception is the octahedral group of order 24 in two variables.

It will be noticed that a transitive group in a prime number of variables n is either primitive or of monomial type. In either case, the corresponding Jordan factor λ must divide the number (4) if $n > 2$.

* See *LGII*, pp. 310, 320-321, and *On Imprimitive Linear Homogeneous Groups*, these Transactions, vol. 6 (1905), p. 232, for an upper limit for all transitive groups. SCHUR has given an upper limit when the weights belong to a given field: Sitzungsberichte der Kgl. Preussischen Akademie der Wissenschaften, 1905, p. 77 ff.

† *LGS*, p. 528.

THE METRICAL ASPECT OF THE LINE-SPHERE TRANSFORMATION*

BY

JULIAN LOWELL COOLIDGE

The line-sphere transformation of Sophus Lie, first described in his remarkable article, "Ueber Complexe, insbesondere Linien und Kugelcomplexe, mit Anwendung auf die Theorie partieller Differentialgleichungen"† derives its interest from two causes. Firstly, lines and spheres are the simplest four-dimensional geometrical manifolds with which we have to deal; it is interesting to establish connections between them. Secondly, intersecting lines correspond to tangent spheres. The consequence usually drawn from this is that the line-sphere transformation falls under the general type of contact transformation, and has the beautiful property of carrying asymptotic lines over into lines of curvature. These facts are of capital importance when the subject is approached from the point of view of Pfaff equations. But we may adopt a different point of view, and then the question naturally arises: "Can not the correspondence of intersecting lines with tangent spheres be made to appear as a special case of some more general relation connecting the distances of lines with the angles of intersection of spheres?" It is the object of the present paper to answer this question affirmatively, to develop as far as possible the relations between the metrical properties of line and sphere systems, and to bring the two into the closest possible connection.‡

Before proceeding to our task, two words of caution are necessary. First, as the angles between spheres appear most naturally through their trigonometric functions, the corresponding line-functions are found most elegantly in non-euclidean space, where distances usually appear in trigonometric form. Secondly, the group of contact transformations that carries lines into lines and keeps distances invariant depends upon six parameters, the group that leaves the angles of spheres intact is a ten parameter group, isomorphic with the quinary orthogonal one. We must, therefore, introduce some seemingly arbitrary restrictions, i. e.,

* Presented to the Society December 29, 1910.

† Mathematische Annalen, vol. 5 (1872).

‡ Since this paper was written my attention has been called to one written in a similar spirit by SEGRE, *Sulle geometrie metriche dei complessi e delle sfere.* Atti della R. Accademia delle Scienze di Torino, vol. 19 (1884). It is to be noted that SEGRE deals with non-oriented spheres, and euclidean line space, so that he is only able to establish a certain similarity in the formulæ, not an identity as in the present case.

assume the invariance of certain additional relations in our sphere system, in order to scale our group down to the proper size.

§ 1. The Line Space Σ.

In a three-dimensional space Σ let a point have four homogeneous coördinates *

$$\xi_0 : \xi_1 : \xi_2 : \xi_3.$$

The system of measurement shall be of the elliptic type, the equation of the Absolute

$$\sum_i^{0\ldots3} \xi_i^2 = 0. \tag{1}$$

The unit of measure shall be so chosen that the distance d of (ξ) and (η) is given by

$$\cos d = \frac{\sum_i^{0\ldots3} \xi_i \eta_i}{\sqrt{\sum_i^{0\ldots3} \xi_i^2} \sqrt{\sum_i^{0\ldots3} \eta_i^2}}. \tag{2}$$

In like manner the angle θ of the two planes

$$\sum_i^{0\ldots3} u_i \xi_i = 0, \qquad \sum_i^{0\ldots3} v_i \xi_i = 0,$$

will have as cosine

$$\cos \theta = \frac{\sum_i^{0\ldots3} u_i v_i}{\sqrt{\sum_i^{0\ldots3} u_i^2} \sqrt{\sum_i^{0\ldots3} v_i^2}}. \tag{3}$$

A line (p) shall be given by its six Plücker coördinates

$$p_{01} : p_{02} : p_{03} : p_{23} : p_{31} : p_{12}, \qquad \rho p_{ij} = \xi_i \eta_j - \xi_j \eta_i = u_k v_l - u_l v_k, \tag{4}$$

where the numbers k, l are complementary to i, j in the system $0, 1, 2, 3$. The polar of (p) with regard to the Absolute, or as we shall say, its *absolute polar* will have the coördinates

$$p'_{ij} = \sigma p_{kl}. \tag{5}$$

The condition for the intersection of two lines (p) and (q) will be

$$\sum_{ijkl}^{0\ldots3} p_{ij} q_{kl} = 0. \tag{6}$$

Each will intersect the polar of the other with regard to the Absolute if

$$\sum_{ij}^{0\ldots3} p_{ij} q_{ij} = 0. \tag{7}$$

* The developments of the present section will be found at greater length in chapters IX, X of the author's *Elements of Non-euclidean Geometry*, Oxford, 1909.

Both expressions will vanish if they intersect orthogonally. A line will touch the Absolute if

$$\sum_{ij}^{0\ldots3} p_{ij}^2 = 0. \tag{8}$$

The expression

$$J = \frac{\sum_{ijkl}^{0\ldots3} p_{ij} q_{kl}}{\sum_{ij}^{0\ldots3} p_{ij} q_{ij}} \tag{9}$$

will be an absolute invariant under the group of all congruent transformations of space. What will be its meaning?

Two lines in elliptic space have two distances, the distances of their intersections with either of the two lines that cut them both orthogonally. They have also two angles, the angles of the pairs of planes determined by the given lines and by each of these perpendiculars. Let one perpendicular cut the two lines in (ξ) and (ξ'), the other cutting them in (η) and (η'). We have for the product of the cosines of the distances d_1 and d_2 of the lines

$$\cos d_1 \cos d_2 = \frac{\sum_{i}^{0\ldots3} \xi_i \xi_i' \sum_{i}^{0\ldots3} \eta_i \eta_i'}{\sqrt{\sum_{i}^{0\ldots3} \xi_i^2} \sqrt{\sum_{i}^{0\ldots3} \eta_i^2} \sqrt{\sum_{i}^{0\ldots3} \xi_i'^2} \sqrt{\sum_{i}^{0\ldots3} \eta_i'^2}}.$$

Now, since the pair $(\xi)(\xi')$ are orthogonal to $(\eta)(\eta')$, i. e., each point lies in the absolute polar plane of each point of the other pair; therefore

$$\sum_{i}^{0\ldots3} \xi_i \eta_i = \sum_{i}^{0\ldots3} \xi_i \eta_i' = \sum_{i}^{0\ldots3} \xi_i' \eta_i = \sum_{i}^{0\ldots3} \eta_i' \eta_i' = 0,$$

$$\sum_{ij}^{0\ldots3} p_{ij} p'_{ij} = \sum_{i}^{0\ldots3} \xi_i \xi_i' \sum_{i}^{0\ldots3} \eta_i \eta_i',$$

$$\sum_{ij}^{0\ldots3} p'^2_{ij} = \sum_{i}^{0\ldots3} \xi_i^2 \sum_{i}^{0\ldots3} \eta_i^2,$$

$$\cos d_1 \cos d_2 = \frac{\sum_{ij}^{0\ldots3} p_{ij} p'_{ij}}{\sqrt{\sum_{ij}^{0\ldots3} p_{ij}^2} \sqrt{\sum_{ij}^{0\ldots3} p'^2_{ij}}}.$$

For the product of the sines of the distances we have likewise

$$\sin d_1 \sin d_2 = \frac{\sqrt{\sum_{i}^{0\ldots3} \xi_i^2 \sum_{i}^{0\ldots3} \xi_i'^2 - \left(\sum_{i}^{0\ldots3} \xi_i \xi_i'\right)^2} \sqrt{\sum_{i}^{0\ldots3} \eta_i^2 \sum_{i}^{0\ldots3} \eta_i'^2 - \left(\sum_{i}^{0\ldots3} \eta_i \eta_i'\right)^2}}{\sqrt{\sum_{i}^{0\ldots3} \xi_i^2} \sqrt{\sum_{i}^{0\ldots3} \eta_i^2} \sqrt{\sum_{i}^{0\ldots3} \xi_i'^2} \sqrt{\sum_{i}^{0\ldots3} \eta_i'^2}},$$

$$\left[\sum_{ijkl}^{0\ldots3}(p_{ij}p'_{kl})\right]^2=|\xi\eta\xi'\eta'|^2$$

$$=\left[\sum_{i}^{0\ldots3}\xi_i^2\sum_{i}^{0\ldots3}\xi_i'^2-\left(\sum_{i}^{0\ldots3}\xi_i\xi_i'\right)^2\right]\left[\sum_{i}^{0\ldots3}\eta_i^2\sum_{i}^{0\ldots3}\eta_i'^2-\left(\sum_{i}^{0\ldots3}\eta_i\eta_i'\right)^2\right],$$

therefore,

$$J\equiv\frac{\sin d_1\sin d_2}{\cos d_1\cos d_2}=\tan d_1\tan d_2. \tag{10}$$

We may say, in particular: for oblique intersection, J vanishes; for the intersection of each line with the absolute polar of the other, J is infinite; for orthogonal intersection, J is indeterminate; when the two distances of the lines are complementary, J equals unity.

The angles of two planes are equal to the distances of their absolute polar lines. But our expression (9) is unaltered if each Plücker coördinate be replaced by its complementary. Hence also

$$J=\tan\theta_1\tan\theta_2. \tag{11}$$

The first interpretation is, however, the one which we shall follow in the present paper.

Two lines shall be said to be *parallel* * when they intersect in a point of the Absolute, they are *pseudo-parallel* † if they lie in a plane tangent to the Absolute. The necessary and sufficient condition for the existence of one of these relations is that the lines should intersect, and that there should be only one line of their pencil tangent to the Absolute,

$$\sum_{ijkl}^{0\ldots3}p_{ij}q_{kl}=\sum_{ij}^{0\ldots3}p_{ij}^2\sum_{ij}^{0\ldots3}q_{ij}^2-\left(\sum_{ij}^{0\ldots3}p_{ij}q_{ij}\right)^2=0. \tag{12}$$

Two lines shall be said to be *paratactic* ‡ if they intersect the same two generators of the same system of the Absolute. What are the Plücker coördinates of such a generator?

The coördinates of a point of the Absolute may be expressed thus,

$$\xi_0:i\xi_1:\xi_2:i\xi_3=(\lambda_1\mu_1-\lambda_2\mu_2):(\lambda_1\mu_1+\lambda_2\mu_2):(\lambda_1\mu_2+\lambda_2\mu_1):(\lambda_1\mu_2-\lambda_2\mu_1).$$

The Plücker coördinates of the generators of one set, which, for definiteness

* This is Lobachevski's form of parallelism.

† This word seems to have been coined by STUDY, *Ueber Nicht-Euklidische und Linien Geometrie*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 15 (1906), pp. 489-490.

‡ The more usual name is *Clifford Parallel*. For "parataxy" see STUDY, loc. cit., or another article of same title, ibid., vol. 8 (1902), p. 317.

we shall call the *left*, will be

$$(13)\quad l_{01}=l_{23}=2\lambda_1\lambda_2,\qquad l_{02}=l_{31}=i(\lambda_1^2+\lambda_2^2),\qquad l_{03}=l_{12}=(\lambda_1^2-\lambda_2^2);$$

the *right* generators may similarly be written

$$(14)\quad r_{01}=-r_{23}=2\mu_1\mu_2,\qquad r_{02}=-r_{31}=i(\mu_1^2+\mu_2^2),\qquad r_{03}=-r_{12}=-(\mu_1^2-\mu_2^2).$$

Two lines (p) and (p') will be *left* paratactic if

$$(15)\quad \begin{aligned} p_{01}+p_{23}&=\rho(p'_{01}+p'_{23}),\\ p_{02}+p_{31}&=\rho(p'_{02}+p'_{31}),\\ p_{03}+p_{12}&=\rho(p'_{03}+p'_{12}). \end{aligned}$$

For *right* parataxy we have similarly

$$(16)\quad \begin{aligned} p_{01}-p_{23}&=\sigma(p'_{01}-p'_{23}),\\ p_{02}-p_{31}&=\sigma(p'_{02}-p'_{31}),\\ p_{03}-p_{12}&=\sigma(p'_{03}-p'_{12}). \end{aligned}$$

For parataxy, right or left, we have

$$(17)\quad \left[\sum_{ijkl}^{0\ldots3} p_{ij}p'_{kl}\pm\sum_{ij}^{0\ldots3}p_{ij}p'_{ij}\right]^2=\left[\sum_{ij}^{0\ldots3}p_{ij}^2\right]\left[\sum_{ij}^{0\ldots3}p'^2_{ij}\right],$$

and from this equation it will appear that when two lines are paratactic, their distances and angles are equal. Conversely, when the distances are equal

$$\frac{\sum_{i}^{0\ldots3}\xi_i\xi'_i}{\sqrt{\sum_{i}^{0\ldots3}\xi_i^2}\sqrt{\sum_{i}^{0\ldots3}\xi'^2_i}}=\frac{\sum_{i}^{0\ldots3}\eta_i\eta'_i}{\sqrt{\sum_{i}^{0\ldots3}\eta_i^2}\sqrt{\sum_{i}^{0\ldots2}\eta'^2_i}}=\frac{\sum_{i}^{0\ldots3}(\rho\xi_i+\sigma\eta_i)(\rho\xi'_i+\sigma\eta'_i)}{\sqrt{\sum_{i}^{0\ldots2}(\rho\xi_i+\sigma\eta_i)^2}\sqrt{\sum_{i}^{0\ldots2}(\rho\xi'^2_i+\sigma\eta'_i)^2}}.$$

There are thus ∞ pairs of points whose distances are the distances of the lines, the lines have ∞^1 common perpendiculars, and so are paratactic.

It is better for our present purpose not to use Plücker coördinates, but the Klein coördinates related to them as follows:

$$(18)\quad \begin{aligned} p_{01}&=\rho(x_0+ix_3), & p_{23}&=\rho(x_0-ix_3),\\ p_{01}&=\rho(x_1+ix_4), & p_{31}&=\rho(x_1-ix_4),\\ p_{03}&=\rho(x_2+ix_5), & p_{12}&=\rho(x_2-ix_5). \end{aligned}$$

Here i is a square root of -1 whose value is supposed to be well determined.

We have then

$$
\begin{aligned}
x_0 &= \sigma(p_{01}+p_{23}), & x_3 &= \sigma i(p_{01}-p_{23}),\\
x_1 &= \sigma(p_{02}+p_{31}), & x_4 &= \sigma i(p_{02}-p_{31}),\\
x_2 &= \sigma(p_{03}+p_{12}), & x_5 &= \sigma i(p_{03}-p_{12}).
\end{aligned} \tag{19}
$$

The coördinates $x_0 : x_1 : x_2$ are proportional to the three non-vanishing Plücker coördinates of the lines through $(1, 0, 0, 0)$ left paratactic to the given line, while $x_3 : x_4 : x_5$ are thenon-vanishing coördinates of the right paratactic through the same point. We get the Absolute polar of a given line by changing the signs of the first three, or last three Klein coördinates; it will be more convenient to adopt the latter alternative. Let us write our general scheme of formulæ in the new coördinates. Intersection of two lines:

$$x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 + x_5y_5 \equiv (xy) = 0, \qquad (xx) \equiv (yy) \equiv 0.$$

Each intersects the absolute polar of the other if

$$x_0y_0 + x_1y_1 + x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 \equiv (x|y) = 0,$$

$$J = \frac{(xy)}{(x|y)}.$$

Orthogonal intersection:

$$(xy) = (x|y) = 0.$$

Parallelism or pseudo-parallelism:

$$(xy) = (x|x)(y|y) - (x|y)^2 = 0.$$

Right parataxy:

$$x_3 = y_3, \qquad x_4 = y_4, \qquad x_5 = y_5.$$

Left parataxy:

$$x_0 = y_0, \qquad x_1 = y_1, \qquad x_2 = y_2.$$

Parataxy in general:

$$[(xy) \pm (x|y)]^2 = (x|x)^2(y|y)^2.$$

Left generators of Absolute:

$$x_3 = x_4 = x_5 = 0.$$

Right generators of Absolute:

$$x_0 = x_1 = x_2 = 0.$$

We shall refer to these formulæ as set (20).

§ 2. Sphere Space S.

In a three-dimensional euclidean space S let a point have the homogeneous rectangular cartesian coördinates $x : y : z : t$. The equation of any sphere may be written

$$ix_1(x^2+y^2+z^2+t^2)+x_2(x^2+y^2+z^2-t^2)+x_3(2x)+x_4(2y)+x_5(2z)=0. \tag{21}$$

The radius will be

$$r = \frac{\sqrt{\sum_i^{1\ldots5} x_i^2}}{ix_1 + x_2}. \tag{22}$$

The centre will have coördinates

$$x : y : z : t = -x_3 : -x_4 : -x_5 : ix_1 + x_2. \tag{23}$$

Let us next assume that the radius may be either positive or negative, and say that a sphere has been *oriented* when the sign of the radius has been determined. A plane shall be said to be *oriented* if the normals have an assigned sense. Hereafter the words *sphere* and *plane* shall be taken to mean *oriented sphere* and *oriented plane*. Let us write

$$x_0^2 = -(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2), \tag{24}$$

so that

$$r = \frac{ix_0}{ix_1 + x_2}.$$

We see that an oriented sphere has six homogeneous coördinates

$$x_0 : x_1 : x_2 : x_3 : x_4 : x_5, \qquad (xx) \equiv 0.$$

The angle of intersection θ of two non-oriented spheres being given by

$$\cos\theta = \frac{\sum_i^{1\ldots5} x_i y_i}{\sqrt{\sum_i^{1\ldots5} x_i^2}\sqrt{\sum_i^{1\ldots5} y_i^2}},$$

we shall define as the angle of intersection of two oriented spheres (x) and (y)

$$\theta = \cos^{-1}\frac{\sum_i^{1\ldots5} x_i y_i}{-x_0 y_0}. \tag{25}$$

They shall be said to be *tangent* if $\cos^2\theta = 1$ and to *touch* if $\cos\theta = 1$. Two tangent spheres whose radii have like signs will touch if their contact be internal.

If one of the oriented spheres be a plane, (25) will give the angle between the directed normal and the internal direction of the radius, if the latter be positive, otherwise the external direction. If both spheres be planes we have the angle of their directed normals. Let us replace (25) by the more convenient

$$\sin^2\tfrac{1}{2}\theta = \frac{(xy)}{2x_0 y_0}. \tag{26}$$

The condition that two spheres should touch is

$$(xy) = 0. \tag{27}$$

If we reverse the signs of $x_3 : x_4 : x_5$ we get the reflection of the given oriented sphere in the origin. We shall understand by *reflection* of a sphere the operation which replaces each point by its reflection and does not alter the orientation of the radius. If θ' be the angle which each of our spheres makes with the reflection of the other in the origin, we get the fundamental formulæ

$$\sin^2 \tfrac{1}{2}\theta' = \frac{(x\,|\,y)}{x_0 y_0}, \qquad J = \frac{(xy)}{(x\,|\,y)} = \frac{\sin^2 \tfrac{1}{2}\theta}{\sin^2 \tfrac{1}{2}\theta'}. \tag{28}$$

This last equation has a meaning even in the case of null spheres. If two proper spheres have radii r, r_1, while the distance of their centres is d and their angle of intersection is θ,

$$d^2 = r^2 + r_1^2 - 2rr_1 \cos\theta, \qquad d^2 - r^2 = -\frac{x_0^2}{(ix_1 + x_2)^2} + \frac{2\sum_i^{1\ldots 5} x_i y_i}{(ix_0 + x_1)(iy_0 + y_1)}.$$

When the sphere (x) becomes null with a finite centre, the expression on the left is the power of that centre with regard to the other sphere; on the right the first term disappears. Hence when (x) is a null sphere with finite centre, and (y) is a sphere of finite radius, our invariant J is the ratio of the power of the centre of (x) with regard to (y) to its power with regard to the reflection of (y) in the origin. When (y) also becomes a null sphere J is the ratio of the square of the distance of centres of (x) and (y) to the square of the distance of each from the reflection of the other.

This deduction is still at fault if (x) be a null sphere, and (y) a plane. Starting with the case where (x) is a null sphere, and (y) a sphere of finite radius, the power of the centre of (x) with regard to (y) divided by the radius of the latter is

$$\frac{2(xy)}{(ix_1 + x_i)y_0}.$$

The limit of this expression as $iy_1 + y_2 \doteq 0$ is the distance from the centre of (x) to the plane (y). Our invariant J will thus give the distance from the centre of (x) to the plane (y) divided by its distance from the reflection of (y) in the origin. The only cases where there is no geometrical interpretation for J are where either

$$x_0 = ix_1 + x_2 = 0 \qquad \text{or} \qquad y_0 = iy_1 + y_2 = 0.$$

Here one at least of the two spheres is a self perpendicular plane (or the plane at infinity) which does not make any particular angle with any thing, and is not at any particular distance from any point not in itself.

§ 3. Corresponding Expressions.

Σ	S
Line.	Sphere.
Polarization in the Absolute.	Reflection in the origin.

Definition. The non-special linear complex in Σ given by the equation

$$x_0 = 0$$

shall be called the *notable complex*. The line whose Klein coördinates are

$$(0 : i : 1 : 0 : 0 : 0)$$

shall be called the *notable line*. Notice that the notable line belongs to the notable complex.

Line of the notable complex.	Null sphere.
Polar lines with regard to the notable complex.	Spheres differing only in orientation.
Notable line.	Plane at infinity.
Lines meeting notable line.	Planes.
Lines of notable complex meeting notable line.	Self-perpendicular planes.
Product of tangents of distances of two lines, neither of which belongs to notable complex.	*Ratio of square of sine of half-angle of two not null spheres to square of sine of half angle which each makes with the reflection of the other in the origin.*
Product of tangents of distances of line belonging to notable complex but not intersecting notable line, and line neither belonging to complex nor meeting notable line.	*Ratio of power of point with regard to a proper sphere, to its power with regard to the reflection of that sphere in the origin.*
Product of tangents of distances of two lines of notable complex neither of which meets notable line.	*Ratio of square of distance of two points to square of distance of each from the reflection of the other in the origin.*
Product of tangents of distances of line meeting notable line but not belonging to notable complex and line belonging to complex but not meeting notable line.	*Ratio of distance of point from plane to its distance from the reflection of plane in the origin.*

These four correspondences are the most important established in the present paper.

Intersecting lines.	Touching spheres.
Orthogonally intersecting lines.	Touching spheres, each of which touches the reflection of the other.

This last correspondence holds only in the general case. We leave to the reader the task of working out the special cases. Touching planes have the same orientation.

Pencil of lines not belonging to the notable complex.	Pencil of touching spheres.
Pencil of lines of notable complex not meeting notable line.	Pencil of null spheres through an isotropic line.

It will be convenient to call an isotropic or self-perpendicular line an *isotropic* merely. The center of the null sphere on the right will lie on the isotropic. The infinite point of the isotropic will correspond to the line of the pencil that meets the notable line.

Pencil of lines of the notable complex which includes notable line.	Pencil of parallel self-perpendicular planes.

If we consider a point in Σ every line through it intersects every line of the notable complex through that point, and the same is true of the lines in a plane.

Point and polar plane in null system of notable complex.	Spheres containing isotropic.

It is more usual to say that a point in Σ corresponds to an isotropic in S. If this mean that there is a one to one correspondence between them, well and good. But if it mean that the lines through a point are in one to one correspondence with the oriented spheres through an isotropic, it is certainly incorrect. Incidentally let us give the correspondence previously mentioned.

Asymptotic line of a surface.	Line of curvature of a surface.
Quadratic Regulus in notable complex whose lines do not meet notable one.	Points of a circle.
Conjugate regulus.	Spheres through same circle.
Conjugate reguli, not in notable complex.	Conjugate generations of a Dupin cyclide.

There are certain special lines worth remarking.

Left generator of Absolute.	Sphere whose centre is origin.
Right generator of Absolute.	Self-perpendicular plane through origin.
Left paratactic lines.	Spheres of equal radius and centres equidistant from origin.
Right paratactic lines.	Spheres whose centres are collinear with origin.

Theorem 1).

If two not mutually absolute polar lines intersect orthogonally two other such lines, they will be paratactic and have an infinite number of common perpendiculars which are paratactic in the other sense. The latter will generate a regulus, whose conjugate consists of paratactic lines including the original two.

Theorem 1′).

If two spheres, not the reflections of one another in the origin, touch two other such spheres, and their reflections, then either their radii are equal, and their centres equidistant from the origin, or they have their centres collinear with the origin. They will touch an infinite number of other spheres and their reflections in the origin. These will be one generation of an anchor ring whose center is the origin, the conjugate generation will include the original two spheres.

The theorem on the right is intuitively evident if we draw any sort of a picture, that on the left is one of the fundamental propositions in the theory of Clifford parallels. If two quadrics intersect in a pair of generators of one set, they will intersect in a pair of the other set also. If one be the Absolute, we have

Theorem 2).

If one set of generators of a quadric be paratactic, the other set are paratactic in the opposite sense.

Theorem 2′).

If one set of generating spheres of a Dupin cyclide have equal radii, and their centres equidistant from a fixed point, the other set have their centres collinear with this point and vice-versa. The cyclide is, under these circumstances, an anchor ring.

The surface on the left is named after the mathematician to whom we owe parataxy.

Clifford surface.

Anchor ring whose axis passes through the origin.

Theorem 3).

Through a given point and in a given plane there will be, in general, one left and one right paratactic to a given line.

Theorem 3′).

Through a given isotropic two spheres can, in general, be passed having their centres on a given line, and two of equal radius whose centres are equidistant from a given point.

Line tangent to Absolute not at a point of notable line.

Sphere whose centre is at null distance from the origin.

Pencil of tangents to Absolute not at point of notable line.	Pencil of spheres through two isotropics which are in a self-perpendicular plane and reflections of each other in the origin.
Line tangent to Absolute at point of notable line.	Self-perpendicular plane.
Pencil of such lines.	Pencil of parallel self-perpendicular planes.
Point of Absolute and its polar in the notable complex, or plane tangent to Absolute and its pole in notable complex.	Isotropic whose plane with the origin is self-perpendicular.
Parallel or pseudo-parallel lines.	Touching spheres one of whose common isotropics determines, with the origin, a self-perpendicular plane.

We get a good deal of light upon our correspondence by considering the corresponding transformation groups.

Group $g_{15}h_{15}$ of collineations and correlations.	Group $g_{15}h_{15}$ of contact sphere transformations.
Group g_6h_6, where g_6 includes all congruent transformations, and h_6 is product of g_6 and absolute polarization.	Group g_6h_6 keeping invariant the assemblage of all spheres which either have their centres at the origin, or are self-perpendicular planes through the origin.
Group g_6 is composed of sub-group γ_6 which permutes the members of each set of generators of the absolute, and the assemblage η_6 which interchanges the two sets.	Group g_6 is composed of sub-group γ_6 which permutes the spheres whose centres are the origin, and the self-perpendicular planes through that point, and η_6 which interchanges the two systems.
The group γ_6 is the product of two invariant subgroups $\gamma_3\gamma_3'$. The former is the group of left translations, which keep all left generators of the absolute in place, the latter is the group of right translations.	The group γ_6 is the product of two invariant subgroups $\gamma_3\gamma_3'$. The former is the group of all rotations about the origin, the latter carries each sphere into another whose centre is collinear with the given centre and the origin, and leaves each self-perpendicular plane through the origin in place.

§ 4. The Linear Complex.

Suppose that we have in Σ a linear complex,

$$(ax) = 0. \tag{29}$$

The corresponding complex in S may be classified as follows: *

a) $$\sum_i^{1\cdots5} a_i^2 \neq 0,$$

here we may write

$$\frac{a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + a_5x_5}{-ix_0\sqrt{\sum_i^{1\cdots5} a_i^2}} = \frac{a_0}{i\sqrt{\sum_i^{1\cdots5} a_i^2}}.$$

This shows that the spheres of the complex cut the *fundamental sphere* (*or plane*) with coördinates

$$i\sqrt{\sum_i^{1\cdots5} a_i^2} : a_1 : a_2 : a_3 : a_4 : a_5$$

at the fixed angle

$$\cos^{-1}\frac{a_0}{i\sqrt{\sum_i^{1\cdots5} a_i^2}}.$$

b) $$a_0 = 0.$$

The spheres are orthogonal to the fundamental sphere, which is null if $\sum_i^{1\cdots5} a_i^2 = 0$.

c) $$a_0 \neq 0, \qquad ia_1 + a_2 \neq 0, \qquad \sum_i^{1\cdots5} a_i^2 = 0.$$

The ratio of the power of a fixed point to the radius of the sphere is a constant for all spheres of the complex. The fixed point may be taken as the centre of a fundamental null sphere.

d) $$a_0 \neq 0, \qquad ia_1 + a_2 = 0, \qquad \sum_i^{1\cdots5} a_i^2 = 0.$$

Spheres are invariantly related to a certain self-perpendicular plane. It is not easy to give a description of this invariant relation.

e) $$a_0 = a_3 = a_4 = a_5 = 0.$$

The complex of all oriented planes.

f) $$a_1 = a_2 = a_3 = a_4 = a_5 = 0.$$

The complex of all null spheres.

* Conf. Snyder, *Über die linearen Complexe der Lie'schen Kugelgeometrie*, Göttingen, 1895, and P. F. Smith, *On the Surfaces enveloped by Spheres belong into a linear Spherical Complex*, Transactions of the American Mathematical Society, vol. 1 (1900).

This complete classification is by means of invariants of the group of motions and inversions, and not by invariants of our group $g_6 h_6$. Let us seek for another definition of the complex.

In our space $\sum$ let us take the non-special complex (29) and find the polar with regard to the corresponding null system of a line (y). This will be

$$\rho y_i' = (aa) y_i - 2(ay) a_i. \tag{30}$$

When will the lines (y) and (y') also be mutually absolute polar? Clearly they must be polar with regard to the absolute polar complex

$$(a|x) = 0$$

and so the directrices of the linear congruence determined by the two complexes.

Let (r) be the coördinates of a line sought. Then if we write

$$(aa) = h(a|a), \qquad -1 \pm \sqrt{1-h^2} = l. \tag{31}$$

$$r_0 : r_1 : r_2 : r_3 : r_4 : r_5 = (h+l)a_0 : (h+l)a_1 : (h+l)a_2 : (h-l)a_3 : (h-l)a_4 : (h-l)a_5.$$

The two lines found from these equations shall be called the *axes* of the complex, the corresponding spheres, the *axial spheres*. Certain special cases must be taken up at once, as (31) will not always hold.

If the complex be self-polar with regard to the absolute, our method of finding the axes breaks down. We see, in fact

$$a_0 = a_1 = a_2 = 0 \qquad \text{or} \qquad a_3 = a_4 = a_5 = 0.$$

In the former case, from (30) and the relation of the absolute polar lines,

$$y_i - \frac{2(ay)a_i}{(aa)} = -y_i \qquad (i = 3, 4, 5),$$

$$(aa) y_i = (ay) a_i, \qquad y_i = a_i.$$

We may take as an axis any line $(r_0 r_1 r_2 a_3 a_4 a_5)$; in the latter case any line $(a_0 a_1 a_2 r_3 r_4 r_5)$ in other words, any line of a definite paratactic system. If

$$(aa) = 0, \qquad (a|a) \neq 0,$$

the complex is special, and the axes are the line met by all lines of the complex, and its absolute polar. If

$$(aa) \neq 0, \qquad (a|a) = 0, \qquad 1/h = 0,$$

the equations for the axis become

$$r_0 : r_1 : r_2 : r_3 : r_4 : r_5 = a_0 : a_1 : a_2 : ia_3 : ia_4 : ia_5$$

the quantity l/h is replaced by i. If

$$(aa) = (a|a) = 0,$$

the axes are (a) and its absolute polar, two lines touching the absolute at the same point. If $h = 1$, the axes fall together into a right generator of the Absolute. If $h = -1$, the axes fall together into a left generator of the absolute.

We shall mean by a *general* linear complex one which has a single definite pair of axes, not touching the absolute, nor lying therein. In such a case we may write

$$
\begin{aligned}
(rx) &= h(ax) + l(a|x), \\
(r|x) &= h(a|x) + l(ax), \\
(r|r) &= 2l\,[h(aa) - (a|a)], \\
\frac{(rx)}{(r|x)} &= \frac{l}{h} \text{ if } (ax) = 0.
\end{aligned} \tag{32}
$$

Theorem 4).

*A general linear complex may be generated in two different ways by a line so moving that the product of the tangents of its distances from a fixed line is constant. The two fixed lines which may be so used are mutually absolute polar, and the two constants are reciprocals.**

Theorem 4′).

A general linear complex may be generated in two different ways by a sphere so moving that the sine of its half-angle with a given sphere bears a fixed ratio to the sine of its half angle with an equal sphere.

The general linear complex has an interesting sub-class.

General linear complex whose axes belong to the notable complex but do not intersect the notable line.

Complex of spheres with regard to which two fixed points have powers in a constant ratio.

The absolute invariant l/h has, in Σ a most interesting significance. Suppose that the axes are the two lines $\xi_0 = \xi_1 = 0$ and $\xi_2 = \xi_3 = 0$. Let us take an infinitesimal screw motion about them

$$
\begin{aligned}
\xi_0' &= \xi_0 + \xi_1 d\theta, \\
\xi_1' &= -\xi_0 d\theta + \xi_1, \\
\xi_2' &= \xi_2 + \xi_3 d\phi, \\
\xi_3' &= -\xi_2 d\phi + \xi_3.
\end{aligned}
$$

The expression $d\phi/d\theta$ will be the *pitch* of the screw with regard to $\xi_0 = \xi_1 = 0$.

* A similar theorem will hold for the linear complex in euclidean space, see SEGRE loc. cit.

If (η) be a point of the absolute polar of the line $(\xi)(\xi')$

$$\sum_{i}^{0\ldots3} \xi_i \eta_i = \sum^{0\ldots3} \xi'_i \eta_i = 0,$$

$$(\xi_0\eta_1 - \xi_1\eta_0)d\theta + (\xi_2\eta_3 - \xi_3\eta_2)d\phi = 0.$$

A line through (ξ) perpendicular to the direction of instantaneous motion will belong to the linear complex

$$p_{01}d\theta + p_{23}d\phi = 0, \qquad (d\theta + d\phi)x_0 + i(d\theta - d\phi)x_3 = 0.$$

This axis of the complex has the coördinates

$$(1:0:0:-i:0:0), \qquad \frac{(rx)}{(r\,|\,x)} = -\frac{d\phi}{d\theta}.$$

Theorem 5). *In a general linear complex the product of the tangents of the distances of the lines from an axis is equal numerically to the pitch, with regard to that axis, of the instantaneous screw motion associated with the complex.*

It will thus be convenient to define our invariant as the *pitch* of the complex. Let us revert to (32). These equations were independent of the relation $(xx) \equiv 0$.

$$\begin{aligned} (ar) &= h(aa) + l(a\,|\,a), \\ (a\,|\,r) &= h(a\,|\,a) + l(aa), \\ (r\,|\,r) &= 2l[h(aa) - (a\,|\,a)]. \end{aligned} \tag{33}$$

Now let (y) and (y') be two lines mutually polar with regard to the complex (i. e., polar with regard to the accompanying null system). We get from (30)

$$\begin{aligned} (ry') &= (aa)(ry) - 2(ay)(xr) \\ &= -(ay)[2l(a\,|\,a) + h(xa)] + l(aa)(a\,|\,y), \\ (r\,|\,y') &= (aa)(r\,|\,y) - 2(ay)(r\,|\,r) \\ &= -(ay)[l(aa) + 2h(a\,|\,a)] + h(aa)(a\,|\,y), \\ \frac{(ry)}{(r\,|\,y)} &= \frac{h(ay) + l(a\,|\,y)}{l(ay) + h(a\,|\,y)}, \\ \frac{(ry')}{(r\,|\,y')} &= \frac{[2l(a\,|\,a) + h(aa)](ay) - l(aa)(a\,|\,y)}{[2h(a\,|\,a) + l(aa)](ay) - h(aa)(a\,|\,y)}. \end{aligned}$$

Eliminating $(ay)/(a\,|\,y)$, and remembering that

$$(aa) = h(a\,|\,a), \qquad h^2 + l^2 = -2l,$$

we have

$$\frac{(ry')}{(r\,|\,y')}\cdot\frac{(ry)}{(r\,|\,y)}=\frac{l^2}{h^2}. \tag{34}$$

Let us also remember that two lines which are mutually polar with regard to a linear complex lie with the axes upon a quadratic regulus.

Theorem 6).

The polar of a line with regard to a general linear complex lies with it and the axes on a quadratic regulus, and the product of the tangents of the distances from an axis to two such polar lines is the square of the corresponding pitch of the complex.

Theorem 6′).

The polar of a sphere with regard to a general linear complex lies with it and the axial spheres in one generation of a Dupin cyclide, and the product of the squared sines of the half angles which two such polar spheres make with one axial sphere divided by the corresponding product for the other axial sphere is the square of the pitch of the complex.

Unfortunately a line is not uniquely determined if we know a regulus whereon it lies, and the product of the tangents of its distances from a line of the regulus. Nevertheless, this theorem enables us quickly to determine the coördinates of the polar of a line with regard to a linear complex. If the axes be (r) and (r') any regulus containing them may be written

$$x_i=\rho^2 r_i+2\rho\sigma s_i+\sigma^2 r_i'.$$

$$(rr)=(r'r')=(rs)=(r's)=(ss)-(rr')=0,\qquad (rr')=(r\,|\,r).$$

If (y) and (y') be polar lines with regard to the complex

$$\frac{(ry')}{(r\,|\,y')}\cdot\frac{(ry)}{(r\,|\,y)}=\frac{\sigma'^2}{\rho'^2}\cdot\frac{\sigma^2}{\rho^2}=\frac{l^2}{h^2},\qquad \frac{\sigma'}{\rho'}\cdot\frac{\sigma}{\rho}=\pm\frac{l}{h}.$$

We must choose the upper sign, as we see by a continuous change from the case where (y) and (y') fall together. When all quantities and all lines here involved are real, the two polar lines will be separated in the regulus by the axes if $l/h<0$ and not separated if $l/h>0$.

Suppose that we have two linear complexes

$$(ax)=0,\qquad (a'x)=0.$$

They have several absolute simultaneous invariants of which the simplest is

$$\frac{(aa')}{(a\,|\,a')},$$

$$r_0=(h+l)a_0,\ \cdots,\ r_3=(h-l)a_3,$$

$$r_0' = (h' + l')a_0' \cdots r_3' = (h' - l')a_3',$$

$$(rr') = (hh' + ll')(ab) + (hl' + lh')(a\,|\,b),$$

$$(r\,|\,r') = (hh' + ll')(a\,|\,b) + (hl' + lh')(ab),$$

$$\frac{(aa')}{(a\,|\,a')} = \frac{\dfrac{(rr')}{(r\,|\,r')}(hh' + ll') - (hl' + lh')}{(hh' + ll') - \dfrac{(rr')}{(r\,|\,r')}(hl' + lh')}.$$

If we write

$$\frac{l}{h} = p, \qquad \frac{l'}{h'} = p',$$

$$\frac{(ab)}{(a\,|\,b)} = \frac{\dfrac{(rr')}{(r\,|\,r')}(1 + pp') - (p + p')}{(1 + pp') - \dfrac{(rr')}{(r\,|\,r')}(p + p')}.$$

Theorem 7)

Two general linear line complexes are in involution if the product of the tangents of the distances of two axes is equal to the sum of pitches divided by the product thereof plus one.

Theorem 7′)

Two general linear sphere complexes are in involution if the square of the sine of the half angle formed by an axial sphere in each, divided by the square of the sine of the half angle of the other axial spheres, is equal to the sum of the corresponding pitches divided by the product thereof plus one.

Let us look briefly at the hitherto excluded case of the complex which is its own absolute polar. Here in S we have ∞^2 axial spheres which either have the same radius and their centers at the same distance from the origin, or all have their centers on one line through the origin. In the former case the complex is transformed into itself by any rotation about the origin, in the latter by any transformation of γ_3'. In the former case we shall have a pitch -1. For if the axis will be $a_0 : a_1 : a_2 : r_3 : r_4 : r_5$

$$(rx) + (r\,|\,x) = 2(ax) = 0.$$

If (x) be a line of the complex

$$\frac{(rx)}{(r\,|\,x)} = -1.$$

The centre of a radical sphere will have the coördinates

$$\frac{-r_3}{ia_1+a_1}, \qquad \frac{-r_4}{ia_1+a_1}, \qquad \frac{-r_5}{ia_1+a_1}.$$

The square of its distance from the origin will be

$$\frac{-(a_0^2+a_1^2+a_2^2)}{(ia_0+a_1)^2} \qquad \text{since} \qquad (rr)=0.$$

The radius of this sphere is

$$\frac{ia_0}{(ia_1+a_2)}.$$

The power of the origin with regard to this sphere is

$$\frac{-(a_1^2+a_2^2)}{(ia_1+a_2)^2},$$

and this is the square of the radius of the fundamental sphere.

Theorem 8). *When the centre of the fundamental sphere is midway between the centres of the axial spheres, the former cuts the latter orthogonally, and the pitch of the complex is equal to* -1.

Suppose next that

$$a_0=a_1=a_2=0.$$

The axial spheres will be any two spheres, symmetrical with regard to the origin,

$$r_0 : r_1 : r_2 : a_3 : a_4 : a_5, \qquad (rr)=0,$$

$$\frac{(rx)}{(r\,|\,x)}=1.$$

The radical plane of the two axial spheres is $0:0:0:a_3:a_4:a_5$.

Theorem 9). *When the fundamental sphere is the radical plane of the axial spheres, the latter may be replaced by any other two spheres symmetrical with regard to the origin, and having the same line of centers, and the pitch of the complex equals* 1.

As a matter of fact we have a great deal more freedom in choosing our axial spheres in the present case, for, as the complex consists in the assemblage of all spheres orthogonal to the fundamental plane, it will be carried into itself by every translation parallel to this plane. We see, more generally, that when the spheres of the complex cut the fundamental sphere orthogonally they make equal angles with any two spheres mutually inverse with regard to the fundamental sphere.

Any linear complex which is not special may be carried into the complex $x_0=0$ by a transformation of the group g_{15}.

Theorem 10).
The intersection of two linear complexes is a linear congruence whose directrices are mutually polar with regard to both.

Theorem 10′).
The locus of points whose powers with regard to two equal spheres have a constant ratio is two spheres differing only in orientation.

The theorem on the right is, of course, true when the two spheres are unequal in radius. It is interesting that there should be a connection between two such well known, but, apparently dissimilar theorems.

There are ∞^1 linear complexes which contain all the lines of a linear congruence.

Theorem 11).
If a linear congruence be given whose directrices are not mutually absolute polar, we may in ∞^2 ways find two lines such that the product of the tangents of the distances from each to the lines of the congruence is constant.

Theorem 11′).
If a system of spheres be given touching two spheres, we may in ∞^5 ways find two pairs of spheres symmetrical with regard to a fixed point so that the ratio of the sines of the half-angles made by the spheres of the system with the two spheres of each pair is constant.

The increased freedom on the right is owing to our ability to choose the origin at will. Let us see if we can not make use of our freedom so that the two constants shall both be equal to 1. Let the given complexes be

$$(ax) = 0, \qquad (bx) = 0.$$

The roots of the quadratic equation

$$(35) \quad \lambda^2[(aa) + (a|a)] + 2\lambda\mu[(ab) + (a|b)] + \mu^2[(bb) + (b|b)] = 0,$$

will, in general, be distinct and give two complexes with different axes.

Theorem 12).
If a linear congruence be given we may, in general, find two not mutually absolute polar lines such that the two distances from each to every line of the congruence are complementary.

Theorem 12′).
If a system of spheres be given touching two spheres we may find two pairs of spheres symmetrical with regard to any point in general position, so that the spheres of the system make equal angles with the two spheres of each pair.

On the right a point "in general position" means one not on the locus that would give the quadratic equation (35) equal roots.

If we have a quadratic regulus given by

$$(ax) = (bx) = (cx) = 0,$$

we may in ∞^3 ways find three sets of roots for the equation

$$\begin{aligned}(36)\qquad &\lambda^2[(aa)+(a|a)]+\mu^2[(bb)+(b|b)]+\nu^2[(cc)+(c|0)]\\ &+2\mu\nu[(bc)+(b|c)]+2\nu\lambda[(ca)+(c|a)]+2\lambda\mu[(ab)+(a|b)]=0.\end{aligned}$$

Theorem 13).
A regulus may be generated in ∞^3 ways by lines whose two distances from each of three fixed lines, no two of which are mutually absolute polar, are complementary.

Theorem 13′).
A generation of a Dupin cyclide may be formed in ∞^6 ways by spheres cutting at equal angles the two spheres of each of three pairs symmetrical with regard to a fixed point.

§ 5. The Dual Projective Geometry.

Let us return to our fundamental equations (31) which may be rewritten

$$r_0 : r_1 : r_2 : r_3 : r_4 : r_5 = a_0 : a_1 : a_2 : \frac{h-l}{h+l}a_3 : \frac{h-l}{h+l}a_4 : \frac{h-l}{h+l}a_5,$$

$$(37)\qquad \frac{h-l}{h+l} = \frac{(aa)+(a|a)\mp\sqrt{(a|a)^2-(aa)^2}}{(aa)-(a|a)\pm\sqrt{(a|a)^2-(aa)^2}} = \pm\frac{\sqrt{(a|a)+(aa)}}{\sqrt{(a|a)-(aa)}}.$$

If, now, we leave $a_0 : a_1 : a_2$ invariant, but change $a_3 : a_4 : a_5$ into $\rho a_3 : \rho a_4 : \rho a_5$, we see that the two axes (r) are unaltered. We have thus ∞^1 complexes which have the same axes or axial spheres, and are said to be *coaxal*. We may thus conceive the two axes or axial spheres as a new space element, determined by two triads of separately homogeneous coördinates.

Theorems 14 and 14′). *There is a one to one correspondence between the pairs of points of two planes (projectively defined), the pairs of lines mutually polar with regard to a quadric and the pairs of spheres symmetrical with regard to a fixed point.*

The system of geometry with any one of these as element may be called *dual projective*. The case where the element is the pair of axes of a coaxal system of

complexes has already been treated at length.* Let us therefore confine ourselves to the relation between the geometry of point-pairs in two projective planes, and pairs of spheres symmetric with regard to a fixed point.

We must begin by taking account of the lapses in the one to one correspondence described in theorem 14. Let us call the plane $a_0 : a_1 : a_2$ the *left plane* while $a_3 : a_4 : a_5$ is the *right plane*. The conics

$$a_0^2 + a_1^2 + a_2^2 = 0, \qquad a_3^2 + a_4^2 + a_5^2 = 0,$$

shall be called the *fundamental conics*. Suppose, first, that the spheres coalesce into a self-perpendicular plane through the origin

$$r_0 = r_1 = r_2 = (rr) = 0.$$

To this will correspond every pair of points

$$(a_0 a_1 a_2), \qquad (r_3 r_4 r_5), \qquad a_0^2 + a_1^2 + a_2^2 \neq 0.$$

We see thus, that to a self-perpendicular plane through the origin will correspond any point in the left plane, not on the fundamental conic, and a definite point of the fundamental conic in the right plane. In the same way, to a sphere whose center is the origin will correspond a definite point of the fundamental conic in the left plane, and any point not on the fundamental conic in the right.

Suppose, thirdly, that we have

$$r_0^2 + r_1^2 + r_2^2 = r_3^2 + r_4^2 + r_5^2 = 0.$$

Every complex of the coaxal system is special, and the spheres form a pencil of tangent spheres through two isotropics, the reflections of each other in the origin, their plane being self perpendicular. Such a pencil will correspond to each pair of points on the two fundamental conics. Conversely if the point in neither plane lie on the fundamental conic, we have a single pair of spheres. We have also a single pair of coincident spheres when one point lies on a fundamental conic and the other does not. When both points lie on the fundamental conics

* The euclidean case was treated first, and at great length, by STUDY in the third part of his *Geometrie der Dynamen*, Leipzig, 1903. The same writer sketched out the non-euclidean cases without proofs in an article *Zur Nichteuklidischen und Liniengeometrie*, Jahresbericht der Deutschen Mathematikervereinigung, vol. 11 (1902). The elliptic case was then studied in detail by the author in his *Dual Projective Geometry of Elliptic and Spherical Space*, Greifswald, 1904, and the hyperbolic by BECK, *Die Strahlenketten im hyperbolischen Raume*, Hannover, 1905. For a briefer account of the non-euclidean cases see the author's *Non-Euclidean Geometry*, already cited, Ch. X.

we have a pencil of spheres through two parallel isotropics the reflections of each other in the origin and in a self-perpendicular plane through the origin.

Before discussing figures generated by sphere-pairs, let us notice that our dual coördinates $(a_0 a_1 a_2)(a_3 a_4 a_5)$ are capable of another interpretation besides that of the system of coaxal complexes. It is, in fact, immediately evident that

$$\frac{a_3}{\sqrt{a_3^2 + a_4^2 + a_5^2}}, \quad \frac{a_4}{\sqrt{a_3^2 + a_4^2 + a_5^2}}, \quad \frac{a_5}{\sqrt{a_3^2\, a_4^2 + + a_5^2}},$$

are the direction cosines of the line of centers of the two spheres. On the other hand if θ_1 and θ_2 be the angles which the two spheres make with the spheres $(i10000)$, $(i01000)$ whose common center is the origin,

$$a_0 : a_1 : a_2 = 1 : i \cos \theta_1 : i \cos \theta_2.$$

The fundamental relation in dual sphere geometry is touching. If

$$u_0 a_0 + u_1 a_1 + u_2 a_2 = 0, \qquad v_3 a_3 + v_4 a_4 + v_5 a_5 = 0,$$

the two spheres $(a_0 a_1 a_2)\,(a_3 a_4 a_5)$ touch the two spheres $(u)\,(v)$.

Suppose that we have a fixed point in one plane, and the points of a line in the other. We have ∞^1 spheres touching a pair of axial spheres, and with their centres either on a line through the origin, or on a sphere whose center is the origin, and with equal radii.

Representing Planes.	S.
Point in one plane not on fundamental conic and line in the other not tangent to the fundamental conic.	One generation of anchor ring whose centre is the origin.
Polar and pole with regard to fundamental conics of foregoing point and line.	Other generation of same ring.

The next most interesting one-parameter family is given by two projective ranges in the two planes

$$a_i = \lambda b_i + \mu c_i, \qquad i = 0, 1, 2, 3, 4, 5. \tag{38}$$

There are three sub-cases.

a) The points of the fundamental conics correspond. We may imagine that these are (b) and (c). Let (r) and (r') be any two spheres of the system.

$$(aa) = 2\lambda\mu(bc), \qquad (a'a') = 2\lambda'\mu'(bc),$$

$$(a\,|\,a) = 2\lambda\mu(b\,|\,c), \qquad (a'\,|\,a') = 2\lambda'\mu'(b\,|\,c),$$

$$h = \frac{(bc)}{(b\,|\,c)} = h', \qquad l = l',$$

$$(rr') = (hh' + ll')(aa') + (hl' + lh')(a\,|\,a'),$$

$$= (h^2 + l^2)(\lambda\mu' + \lambda'\mu)(bc) + 2hl(\lambda\mu' + \lambda'\mu)(b\,|\,c),$$

$$= 0, \qquad \text{since } h^2 + l^2 = -2l.$$

Projective ranges where the points of fundamental conics correspond.	Pencil of mutually touching spheres which touch two axial spheres.

b) One intersection with a fundamental conic corresponds to one such in the other plane. This is an unsymmetrical case which we pass over.

c) The intersections with the fundamental conics do not correspond.

The one parameter family of spheres all touch a pair of axial spheres and generate a surface which we shall call a C surface. Let us find its order. If

$$\lambda/\mu = z,$$

$$(aa) = z^2(bb) + 2z(bc) + (cc),$$

$$(a\,|\,a) = z^2(b\,|\,b) + 2z(b\,|\,c) + (c\,|\,c),$$

$$r_0 = \sqrt{[(bb) - (b\,|\,b)]z^2 + 2[(bc) - (b\,|\,c)]z + [(cc) - (c\,|\,c)]}\,(zb_0 + c_0),$$

$$r_3 = \sqrt{[(bb) + (b\,|\,b)]z^2 + 2[(bc) + (b\,|\,c)]z + [(cc) + (c\,|\,c)]}\,(zb_3 + c_3),$$

$$r_0 = \sqrt{f_2(z)}(zb_0 + c_0), \qquad \alpha_3 = \sqrt{\phi_2(z)}(zb_4 + c_3).$$

If $0 : x_1 : x_2 : x_3 : x_4 : x_5$ be a point of this sphere

$$\sqrt{f_2(z)} \sum_{i}^{1\ldots2} (zb_i + c_i)x_i + \sqrt{\phi_2(z)} \sum_{i}^{3\ldots5} (zb_i + c_i)x_i = 0.$$

To find the envelop of these spheres we must square this expression getting an expression of the fourth order in z, quadratic in x_i, differentiate with respect to z and eliminate that parameter. This gives an expression of the fourteenth order in x_i.

Theorem 15′. *The surfaces C are of the twenty-eighth order, with the circle at infinity as a curve of the fourteenth order.*

This theorem would be of uncommonly little importance, were it not for a very general and remarkable property of C surfaces. Suppose that we have any analytic congruence of spheres

$$b_i = b_i(uv).$$

Let us find the sphere which touches (b), its adjacent sphere

$$(b) + \frac{\partial (b)}{\partial u} du + \frac{\partial (b)}{\partial v} dv,$$

and the reflections of the two in the origin,

$$a_0 b_0 + a_1 b_1 + a_2 b_2 = a_3 b_3 + a_4 b_4 + a_5 b_5 = 0,$$

$$\sum_i^{0,\dots,2} a_i \left(\frac{\partial b_i}{\partial u} du + \frac{\partial b_i}{\partial v} dv \right) = \sum_i^{3,\dots,5} a_i \left(\frac{\partial b_i}{\partial u} du + \frac{\partial b_i}{\partial v} dv \right) = 0.$$

Let us assume that

$$\begin{vmatrix} a_0 & \frac{\partial b_1}{\partial u} & \frac{\partial b_2}{\partial v} \end{vmatrix} \neq 0, \qquad \begin{vmatrix} a_3 & \frac{\partial b_4}{\partial u} & \frac{\partial b_5}{\partial v} \end{vmatrix} \neq 0.$$

We choose such a (b) (said to be in the general position) that neither of these determinants vanishes. We may then write

$$a_i = du \begin{vmatrix} b_j & b_k \\ \frac{\partial b_j}{\partial u} & \frac{\partial b_k}{\partial u} \end{vmatrix} + dv \begin{vmatrix} b_j & b_k \\ \frac{\partial b_j}{\partial v} & \frac{\partial b_k}{\partial v} \end{vmatrix} \tag{39}$$

where i, j, k are circular permutations of $0, 1, 2$ and $3, 4, 5$. Varying du and dv at will, we have

Theorem 16′. *If an analytic congruence of spheres be given and a point chosen which is neither the vertex of a cone which is the locus of their centres, nor the centre of ∞^1 spheres each passing through the centres of ∞^1 spheres of the congruence of equal radius, then if a sphere of the congruence be chosen, the spheres which touch it and the adjacent spheres of the congruence, as well as the reflections in the fixed point, will generate a C surface.**

An interesting two parameter family is the chain congruence, given by

$$a_i = \lambda b_i + \mu c_i + \nu d_i, \qquad i = 0, 1, 2, \quad \text{or} \quad 3, 4, 5. \tag{40}$$

* This is, of course, the line-sphere transform of the non-euclidean form of Hamilton's famous theorem on the cylindroid. See his paper on *Systems of Rays*, Transactions of the Royal Irish Academy, vol. 15 (1829), and the author's *Non-euclidean Geometry*, chap. X.

We pass over the discussion of the various possible special cases, and take the general case where we can solve three of the equations for λ, μ, ν and substitute in the other three. We may here write

$$a_0 = u_0 a_3, \qquad a_1 = u_1 a_4, \qquad a_2 = u_2 a_5.$$

The spheres which touch two spheres of the congruence and their reflections in the origin will generate the conjugate congruence

$$b_3 = u_0 b_0, \qquad b_4 = u_1 b_1, \qquad b_5 = u_2 b_2.$$

General projectivity between the two planes.	Chain congruence.
Contragredient projectivity.	Conjugate congruence.

When a projective relation is established between two planes, one is thereby established between the ranges on any two corresponding lines in them.

Theorem 17'). *The spheres of a chain congruence which touch one of the conjugate congruence and its reflection in the origin generate a C surface.*

Are there any spheres of our congruence which touch one of the conjugate congruence without touching its reflection? Let us write

$$r_0 = a_0, \qquad r_3 = \frac{h-l}{h+l} a_3, \qquad s_0 = b_0, \qquad s_3 = \frac{h'-l'}{h'+l'} b_3.$$

If $(rs) = 0$,

$$(a_0 b_0 + a_1 b_1 + a_2 b_2)\left[1 + \frac{(h-l)(h'-l')}{(h+l)(h'+l')}\right] = 0.$$

If the first factor vanish (a) touches (b) and also its reflection. If the second vanish

$$hh' + ll' = 0.$$

But there will be a singly infinite set of values for (a) and (b) in the two congruences satisfying that equation. Hence ∞^1 spheres of each congruence touch ∞^1 of the other, but not their reflections.

Theorem 18). *The spheres of a chain congruence which touch a sphere of the conjugate but not its reflection in the origin form one generation of a Dupin cyclide, the other generation belonging to the conjugate congruence.*

Theorem 19). *The spheres which touch pairs of spheres of one generation of a Dupin cyclide and their reflections in a fixed point generate a chain congruence.*

The chain congruence has many other beautiful properties, easily proved from the corresponding properties of the chain congruences of lines by means of the line-sphere transformation.

In closing one remark of a general character may not be out of place. The method of polar reciprocation in a quadric, descriptively considered, is a means of illustrating the principle of duality. Metrically, it shows the perfect correspondence of the concepts of distance and angle in non-euclidean space. The line-sphere transformation, descriptively considered, is one of the most beautiful examples under the general type of contact transformation. Metrically, as we have seen, it brings out numerous relations between the distances of lines and the angles of spheres. Is it not probable that there exists a large class of contact transformations which are not merely descriptive in character, but may be used to establish interesting metrical relations among elements of various sorts? Can we, without a total loss of naturalness, include all contact transformations in such a class?

CAMBRIDGE, MASS.,
July, 1910.

NATURAL SYSTEMS OF TRAJECTORIES GENERATING FAMILIES OF LAMÉ*

BY

EDWARD KASNER

As in the author's previous papers in these Transactions,† the term *natural* is employed to designate those quadruply-infinite systems of space curves which can be identified with the totality of extremals of a variation problem of the form

$$\int F(x, y, z)\,ds = \text{minimum} \qquad (ds^2 = dx^2 + dy^2 + dz^2). \tag{1}$$

Such a system has the characteristic property that if ∞^2 of the curves are orthogonal to one surface they are necessarily orthogonal to ∞^1 surfaces. The equation of these ∞^1 surfaces may be written in the form

$$f(x, y, z) = \text{constant} \tag{2}$$

where f satisfies the Hamilton-Jacobi equation

$$f_x^2 + f_y^2 + f_z^2 = F^2 \tag{3}$$

associated with (1).

A set of ∞^1 surfaces of this sort will be termed a set of wave fronts or, more simply, a *wave set*. The natural system being given, every surface determines one of these wave sets. The phraseology employed is of course suggested by the optical interpretation of (1), in which $F(x, y, z)$ represents the index of refraction in a non-homogeneous isotropic medium: the curves of the natural system are then the possible paths of light; and a disturbance starting from any surface will be propagated by means of a set of wave fronts.

The question arises whether wave sets may be families of Lamé, that is, simply infinite families of surfaces which can form part of a triply-orthogonal system. Ordinarily this is not the case. The condition that (2) shall represent a Lamé family is that f satisfy the Darboux-Cayley equation of third order‡

* Presented to the Society, under a different title, December 29. 1909.

† *Natural families of trajectories: conservative fields of force*, vol. 10 (1909), pp. 201–219; *The theorem of Thomson and Tait and natural families of trajectories*, vol. 11 (1910), pp. 121–140.

‡ DARBOUX, *Leçons sur les systèmes orthogonaux*, vol. 1 (1898), p. 23.

$$\begin{vmatrix} H_{xx} & H_{yy} & H_{zz} & H_{yz} & H_{xz} & H_{xy} \\ f_{xx} & f_{yy} & f_{zz} & f_{yz} & f_{xz} & f_{xy} \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 2f_x & 0 & 0 & 0 & f_z & f_y \\ 0 & 2f_y & 0 & f_z & 0 & f_x \\ 0 & 0 & 2f_z & f_y & f_x & 0 \end{vmatrix} = 0, \tag{4}$$

where

$$H \equiv (f_x^2 + f_y^2 + f_z^2)^{-\frac{1}{2}}. \tag{5}$$

The problem of the present paper is to find those natural systems for which all the associated wave sets are families of Lamé. The solution together with optical and kinetic formulations follow:

THEOREM I. *The only natural systems whose wave sets are of the Lamé type are those composed of the ∞^4 circles orthogonal to a fixed sphere. The corresponding variation problem* (1) *is of the form*

$$\int \frac{ds}{a_0(x^2+y^2+z^2) + a_1x + a_2y + a_3z + a_4} = \text{minimum}.$$

THEOREM II. *The only isotropic media for which every disturbance spreads out by means of a Lamé family of surfaces are those in which the index of refraction is of the form*

$$[\, a_0(x^2+y^2+z^2) + a_1x + a_2y + a_3z + a_4 \,]^{-1};$$

its value at any point varies inversely as the power of that point with respect to a fixed sphere.

THEOREM III. *The only conservative fields of force such that, when the energy constant is taken equal to zero, every set of surfaces of equal action is of the Lamé type, are those in which the potential at any point varies inversely as the square of the power of the point with respect to a fixed sphere.*

The analytic formulation of our problem is as follows: Determine the function F in such a way that every function f which satisfies the Hamilton-Jacobi equation (3) shall also satisfy the Darboux-Cayley equation (4).

It will be convenient to write the former equation in the form

$$f_x^2 + f_y^2 + f_z^2 = 2W, \tag{6}$$

so that

$$2W \equiv F^2. \tag{7}$$

By differentiation, we have

$$
\begin{aligned}
f_x f_{xx} + f_y f_{yx} + f_z f_{zx} &= W_x, \\
f_x f_{xy} + f_y f_{yy} + f_z f_{zy} &= W_y, \\
f_x f_{xz} + f_y f_{yz} + f_z f_{zz} &= W_z.
\end{aligned} \tag{8}
$$

Hence of the six partial derivatives of the second order which appear in (4) we may eliminate say f_{xx}, f_{yy}, f_{zz}. The final result may be put into the form

$$
\begin{vmatrix}
A & B & C & H_{yz} & H_{zx} & H_{xy} \\
W_x & W_y & W_z & f_{yz} & f_{zx} & f_{xy} \\
f_x & f_y & f_z & 0 & 0 & 0 \\
2W & 0 & 0 & 0 & f_z & f_y \\
0 & 2W & 0 & f_z & 0 & f_x \\
0 & 0 & 2W & f_y & f_x & 0
\end{vmatrix} = 0, \tag{9}
$$

where

$$
\begin{aligned}
A &\equiv f_x H_{xx} + f_y H_{xy} + f_z H_{xz}, \qquad B \equiv f_x H_{yx} + f_y H_{yy} + f_z H_{yz}, \\
C &\equiv f_x H_{zx} + f_y H_{zy} + f_z H_{zz},
\end{aligned} \tag{10}
$$

$$
H \equiv (2W)^{-1} \equiv F^{-1}. \tag{11}
$$

Equation (9) may be expanded in the form

$$
\alpha f_{yz} + \beta f_{zx} + \gamma f_{xy} + \delta = 0, \tag{12}
$$

where the coefficients involve only derivatives of first order. Since, in virtue of (8), the quantities f_{yz}, f_{zx}, f_{xy} are numerically arbitrary, it follows that the above coefficients must vanish individually.

It will be sufficient to calculate γ, the minor of f_{xy} in (9). The resulting condition is found to be

$$
f_z\{H_{xy}(f_x^2 - f_y^2) + (H_{yy} - H_{xx}) f_x f_y\} - (f_x^2 + f_y^2)(f_x H_{yz} - f_y H_{xz}) = 0. \tag{13}
$$

This is to hold as a consequence of (6); hence the left hand member of (13), a homogeneous cubic in f_x, f_y, f_z, must be divisible by the non-homogeneous quadratic $f_x^2 + f_y^2 + f_z^2 - 2W$. It follows that (13) must be an identity. Equating the coefficients to zero and adjoining other conditions obtained by cyclic permutation of the letters x, y, z, we find

$$
H_{xx} = H_{yy} = H_{zz}, \qquad H_{yz} = H_{zx} = H_{xy} = 0. \tag{14}
$$

It follows that the function H must be of the form

$$
H = a_0(x^2 + y^2 + z^2) + a_1 x + a_2 y + a_3 z + a_4. \tag{15}
$$

It is easily verified that, for this form of H, equation (9) holds identically and is thus certainly satisfied by all the solutions of (6).

The result of our analytic discussion is that the only cases in which all the solutions of (3) are also solutions of (4) are defined by

$$F = [a_0(x^2 + y^2 + z^2) + a_1 x + a_2 y + a_3 z + a_4]^{-1}. \tag{16}$$

The natural system associated with such a function is easily shown to consist of the ∞^4 circles orthogonal to the fixed sphere S

$$a_0(x^2 + y^2 + z^2) + a_1 x + a_2 y + a_3 z + a_4 = 0. \tag{17}$$

The Lamé families corresponding to the form (15) are well known.* The ∞^1 surfaces of each of these families have for orthogonal trajectories circles orthogonal to S. These circles cut any two of the surfaces and S in four points whose anharmonic ratio is constant.

The ten-parameter group of conformal transformations of space converts natural systems into natural systems and Lamé families into Lamé families; and, therefore, solutions of our problem into solutions. With respect to real transformations there are three types according as the radius of the sphere S is zero, real, or imaginary. The function H may be reduced to one of the forms

$$x^2 + y^2 + z^2, \qquad x^2 + y^2 + z^2 - k^2, \qquad x^2 + y^2 + z^2 + k^2, \tag{18}$$

In the optical interpretation the index of refraction is F or $1/H$. It is thus of one of the forms

$$\frac{1}{r^2}, \qquad \frac{1}{r^2 - k^2}, \qquad \frac{1}{r^2 + k^2}, \tag{19}$$

where r is the distance from the origin and k is a real constant. These three media furnish representations of the parabolic, elliptic, and hyperbolic geometries respectively.

In the kinetic interpretation, the work function W, according to (11), is proportional to H^{-2}, and is thus

$$\frac{1}{r^4}, \qquad \frac{1}{(r^2 - k^2)^2}, \qquad \frac{1}{(r^2 + k^2)^2}. \tag{20}$$

The force is hence central and varies as

$$\frac{1}{r^5}, \qquad \frac{r}{(r^2 - k^2)^3}, \qquad \frac{r}{(r^2 + k^2)^3}. \tag{21}$$

It is to be remembered that the constant of energy must here be taken equal to zero. The dynamical trajectories are then the systems of circles described above. For other values of the energy constant, the trajectories are represented by elliptic functions and the systems do not give rise to Lamé families.

* They were first studied by RIBAUCOUR. Cf. DARBOUX, *loc. cit.*, pp. 53, 56.

It is easily seen that the natural systems obtained are the only ones composed exclusively of circles. This follows from the fact that any family of surfaces whose orthogonal trajectories are circles is necessarily a Lamé family. We thus have

THEOREM IV. *The only natural systems of circles are those formed by the circles orthogonal to a fixed sphere.*

The media (19) are hence the only simply-refracting media in which all light rays are circular.

In conclusion we observe that, since natural systems are characterized by the property of Thomson and Tait,* and Lamé families are characterized by a certain property of Ribaucour,† our first theorem may be restated in the following purely geometric form:

THEOREM V. *If a system of ∞^4 curves in space is to be such that, for an arbitrarily selected surface Σ: 1) there are ∞^2 curves of the system orthogonal to Σ and these form a normal congruence; 2) the osculating circles of these ∞^2 curves for the points of Σ also form a normal congruence; then the system must be composed of the ∞^4 circles orthogonal to a fixed sphere.*‡

Theorem IV is seen to be included in this result as a special case.

COLUMBIA UNIVERSITY, NEW YORK.

* These Transactions, vol. 11 (1910), p. 121.

† DARBOUX, *loc. cit.*, p. 78.

‡ It is sufficient, in fact, to require merely that the osculating circles shall form a normal congruence. That the system is then natural follows from Theorem II, these Transactions, vol. 11 (1910), p. 130.

A FUNDAMENTAL SYSTEM OF INVARIANTS OF THE GENERAL MODULAR LINEAR GROUP WITH A SOLUTION OF THE FORM PROBLEM*

BY

LEONARD EUGENE DICKSON

1. We shall determine m functions which form a fundamental system of invariants for the group G_m of all linear homogeneous transformations on m variables with coefficients in the Galois field of order p^n. In the so-called form problem for the group G_m, we seek all sets of values of the m variables for which the m fundamental absolute invariants take assigned values. It is shown in § 8 that all sets of solutions are linear combinations of the roots of an equation involving only the powers p^{nm}, $p^{n(m-1)}$, $\cdots$, p^n, 1 of a single variable. This fundamental equation has properties analogous to those of a linear differential equation of the m-th order. In §§ 10–16 we determine the degrees of the irreducible factors of the fundamental equation and, in particular, the smallest field in which it is completely solvable. We obtain a wide generalization of the theory of the equation $\xi^{p^m} - \xi = 0$, which forms the basis of the theory of finite fields. The function defined by the left member of the fundamental equation includes the type of substitution quantics in one variable the theory of which is equivalent to, but preceded historically, the theory of linear modular substitutions on m variables. We here find that the latter theory necessitates a return to the earlier quantics in one variable. Finally, in §§ 17–22, we consider the interpretation of certain invariants.

It follows from the theorem concerning the product of two determinants that a transformation T of G_m replaces the function

$$[e_1, \cdots, e_m] = \begin{vmatrix} x_1^{p^{e_1 n}} & x_2^{p^{e_1 n}} & \cdots & x_m^{p^{e_1 n}} \\ x_1^{p^{e_2 n}} & x_2^{p^{e_2 n}} & \cdots & x_m^{p^{e_2 n}} \\ \cdot & \cdot & \cdot & \cdot \\ x_1^{p^{e_m n}} & x_2^{p^{e_m n}} & \cdots & x_m^{p^{e_m n}} \end{vmatrix}$$

by one which equals $|T|$ times the initial function. By § 2, each of these functions has the factor

$$L_m = [m-1, m-2, \cdots, 1, 0].$$

* Presented to the Society, September 6, 1910.

Certain of the quotients will be given a special notation:

$$Q_{ms} = [m, m-1, \cdots, s+1, s-1, \cdots, 1, 0]/L_m.$$

They are absolute invariants of G_m. We shall prove the

Theorem. *The m invariants L_m, Q_{m1}, $\cdots$, $Q_{m\,m-1}$ are independent and form a fundamental system of invariants of the group G_m.*

2. Consider the product P of all the linear functions

$$a_1x_1 + a_2x_2 + \cdots + a_mx_m$$

in which the a_i are elements not all zero of the $GF[p^n]$ and such that, of the coefficients a_i not zero, the one with smallest subscript is unity:

$$P = \prod_{k=1}^{m} \prod_{a} (x_k + a_{k+1}x_{k+1} + \cdots + a_mx_m),$$

where the inner product extends over the $p^{n(m-k)}$ sets $a_{k+1}, \cdots, a_m$ of $m-k$ elements of the field. Hence the term

$$\prod_{k=1}^{m} x_k^{p^{n(m-k)}} = x_1^{p^{n(m-1)}} \cdots x_{m-1}^{p^n} x_m$$

occurs once and but once in the expansion of P and has the coefficient unity. This term is the product of the elements in the main diagonal of the determinant L_m. Since L_m is invariant * under G_m and has the factor x_1, it follows that L_m is identical † with the product P.

Similarly, $[e_1, \cdots, e_m]$ has the factor L_m.

Theory of Ternary Invariants.

3. In the adjoint determinant of the nine first minors of

$$L_3 = (x^{p^{2n}} y^{p^n} z),$$

consider the three determinants formed of the elements in the first and third columns:

$$\begin{vmatrix} (y^{p^n}z) & (x^{p^n}y) \\ (y^{p^{2n}}z^{p^n}) & (x^{p^{2n}}y^{p^n}) \end{vmatrix}, \quad \begin{vmatrix} (y^{p^{2n}}z) & (x^{p^{2n}}y) \\ (y^{p^{2n}}z^{p^n}) & (x^{p^{2n}}y^{p^n}) \end{vmatrix}, \quad \begin{vmatrix} (y^{p^n}z) & (x^{p^n}y) \\ (y^{p^{2n}}z) & (x^{p^{2n}}y) \end{vmatrix}.$$

They equal $y^{p^n}L_3$, $y^{p^{2n}}L_3$, yL_3, respectively. Hence $L_3^{p^n-1}$ times the first determinant equals the p^n-th power of the third. Transposing the negative terms

* This fact appears to have been first noted by the writer. See his *Linear Groups*, p. 216.

† This theorem is due to Professor E. H. MOORE, Bulletin of the American Mathematical Society, vol. 2 (1896), p. 189. His three proofs differ from the above invariantive proof. His sequence of variables is the reverse of that employed here.

and dividing by $(x^{p^{2n}}y^{p^n})(y^{p^{2n}}z^{p^n})$, we get

$$\frac{(y^{p^n}z)L_3^{p^n-1}+(y^{p^{2n}}z^{p^n})}{(y^{p^{2n}}z^{p^n})}=\frac{(x^{p^n}y)L_3^{p^n-1}+(x^{p^{2n}}y^{p^n})}{(x^{p^{2n}}y^{p^n})}.$$

The second member is invariant under G_2 (§ 1) and is replaced by the first member by the transformation $x'=z$, $z'=-x$, which extends G_2 to G_3. Hence the second member is an invariant of G_3.

Similarly, from the first and second determinants, we get

$$\frac{(x^{p^{2n}}y)L_3^{p^n-1}+(x^{p^{2n}}y^{p^{2n}})}{(x^{p^{2n}}y^{p^n})}=\frac{(y^{p^{2n}}z)L_3^{p^n-1}+(y^{p^{2n}}z^{p^{2n}})}{(y^{p^{2n}}z^{p^n})},$$

so that the first member is an invariant of G_3.

If we employ the following integral invariants of G_2,

$$(1)\qquad L_2=(x^{p^n}y),\qquad Q_{21}=\frac{(x^{p^{2n}}y)}{L_2}=\frac{x^{p^{2n}-1}-y^{p^{2n}-1}}{x^{p^n-1}-y^{p^n-1}},$$

we may express our ternary invariants in the form

$$(2)\qquad L_3,\qquad Q_{32}=\left(\frac{L_3}{L_2}\right)^{p^n-1}+Q_{21}^{p^n},\qquad Q_{31}=Q_{21}\left(\frac{L_3}{L_2}\right)^{p^n-1}+L_2^{p^{2n}-p^n},$$

the identification of the last two with the quotients Q_{3i} (§ 1) being made in § 4. The fact that L_3 is divisible by L_2 follows from § 2; the quotient may be obtained from the expansion

$$(3)\qquad L_3=z^{p^{2n}}L_2-z^{p^n}L_2Q_{21}+zL_2^{p^n}.$$

We proceed to the proof that the three invariants (2) form a fundamental system. Let I be any homogeneous ternary invariant and let I_0 be the sum of the terms of I which lack z. Then I_0 and the coefficients of the various powers of z in I are invariants of the binary group G_2 on x, y, and hence* are integral functions of the invariants (1).

Let $cL_2^aQ_{21}^b$ be the term of I_0 in which a is a minimum. Then the term of I_0 of minimum degree in y is cx^ey^a, where

$$e=ap^n+bd,\qquad d=p^{2n}-p^n.$$

Since x^ey^a does not occur elsewhere in I_0, cx^ey^a and therefore also cz^ey^a is a term of I. Hence cy^a is a term of an invariant of G_2 and hence a term of kQ_{21}^α. Thus $a=\alpha d$.

Let $c'L_2^{a'}Q_{21}^{b'}$ be any term of I_0. By the homogeneity of I_0,

$$(a'-a)(p^n+1)+(b'-b)d=0.$$

Hence a' is divisible by p^n. We next show that a' is divisible by p^n-1, so that a' is divisible by $d=p^n(p^n-1)$.

* DICKSON, these Transactions, this volume, p. 1.

Apply to I_0 a transformation of determinant ρ, where ρ is a primitive root of the $GF[p^n]$. Since Q_{21} is an absolute invariant and L_2 takes the factor ρ (§ 1), it follows that $\rho^{a'} = \rho^a$, whence $a' \equiv a \pmod{p^n - 1}$. But a is divisible by d. Hence a' is divisible by $p^n - 1$.

Let $b = p^\beta B$, where B is prime to p. Let $f = p^\beta (p^n - 1)$. Then

$$Q_{21} = x^d + x^{d-p^n+1} y^{p^n-1} + \cdots, \qquad Q_{21}^{p^\beta} = x^{dp^\beta} + x^{dp^\beta - f} y^f + \cdots,$$

$$Q_{21}^b = x^{bd} + Bx^{bd-f} y^f + \cdots,$$

$$L_2^a = (x^{p^{2n}} y^{p^n} - x^{p^n} y^{p^{2n}})^{a(p^n-1)} = x^{ap^n} y^a + \alpha x^{ap^n-d} y^{a+d} + \cdots.$$

Suppose that $\beta < n$. Then $f < d$ and

$$L_2^a Q_{21}^b = x^{\mu+f} y^a + Bx^\mu y^{a+f} + \cdots \qquad (\mu = ap^n + bd - f).$$

Neither of these terms occurs in another term $c' L_2^{a'} Q_{21}^{b'}$, for which therefore $a' > a$. In fact, $a' \geqq a + d > a + f$. Hence I contains the term $cBz^\mu y^{a+f}$. But $a + f$ is not a multiple of d and B is not zero in the field. Hence $\beta \geqq n$ and b is of the form $p^n b_1$. Hence by (2),

$$I' = I - c Q_{31}^a Q_{32}^{b_1}$$

is an invariant in which I_0' lacks $cL_2^a Q_{21}^b$.

We can similarly delete one after another of the terms free of z and reach ultimately an invariant I_1 in which there are no terms free of z. Since I_1 has the factor z, it has the factor L_3. Thus $I_1 = L_3' I_2$, where I_2 is either a constant or else is a function having terms free of z. In the latter case we repeat the above process on I_2. It follows that *any integral invariant of G_3 is an integral function of the three invariants* (2).

4. For $m = 3$, the invariants Q_{ms} of § 1 are

$$Q_{32} = (x^{p^{3n}} y^{p^n} z)/L_3, \qquad Q_{31} = (x^{p^{2n}} y^{p^{2n}} z)/L_3.$$

Their degrees $p^{3n} - p^{2n}$ and $p^{3n} - p^n$ equal the degrees of the second and third invariants (2), respectively. Hence by the theorem of § 4 the corresponding invariants differ only by a constant factor. We now prove that the factor is unity in each case.

The terms free of z in the quotient Q_{3i} are given by the quotient of the coefficient of z in the numerator by the coefficient of z in the denominator L_3. For $i = 2, 1$, we get respectively

$$(x^{p^{3n}} y^{p^n})/(x^{p^{2n}} y^{p^n}) = Q_{21}^{p^n}, \qquad (x^{p^{3n}} y^{p^{2n}})/(x^{p^{2n}} y^{p^n}) = L_2^{p^{2n}-p^n}.$$

Hence the relations (2) are proved. For another proof by means of a vanishing determinant of the fifth order, see § 6.

Expressions for the Quotients Q_{ms}.

5. The process which led so naturally to invariants (2) can be readily applied also when $m > 3$. For example, if $m = 4$,

$$\begin{vmatrix} (x^{p^{2n}} y^{p^n} w) & (x^{p^{2n}} y^{p^n} z) \\ (x^{p^{2n}} y^{p^n} w) & (x^{p^{2n}} y^{p^n} z) \end{vmatrix} = L_4 \begin{vmatrix} x^{p^{2n}} & y^{p^{2n}} \\ x & y \end{vmatrix},$$

$$\begin{vmatrix} (x^{p^{2n}} y^{p^n} w) & (x^{p^{2n}} y^{p^n} z) \\ (x^{p^{3n}} y^{p^{2n}} w^{p^n}) & (x^{p^{3n}} y^{p^{2n}} z^{p^n}) \end{vmatrix} = L_4 \begin{vmatrix} x^{p^{2n}} & y^{p^{2n}} \\ x^{p^n} & y^{p^n} \end{vmatrix}.$$

Equating the p^n-th power of the upper to $L_4^{p^n-1}$ times the lower, transposing the negative terms, and dividing by $(x^{p^{3n}} y^{p^{2n}} w^{p^n})(x^{p^{3n}} y^{p^{2n}} z^{p^n})$, we get

$$\frac{(x^{p^{2n}} y^{p^n} z) L_4^{p^n-1} + (x^{p^{4n}} y^{p^{2n}} z^{p^n})}{(x^{p^{3n}} y^{p^{2n}} z^{p^n})} = \frac{(x^{p^{2n}} y^{p^n} w) L_4^{p^n-1} + (x^{p^{4n}} y^{p^{2n}} w^{p^n})}{(x^{p^{3n}} y^{p^{2n}} w^{p^n})}.$$

It follows that the left member is an invariant of G_4 (later identified with Q_{43}). We are led in a similar manner to the invariants

$$\frac{(x^{p^{3n}} y^{p^n} z) L_4^{p^n-1} + (x^{p^{4n}} y^{p^{3n}} z^{p^n})}{(x^{p^{3n}} y^{p^{2n}} z^{p^n})}, \qquad \frac{(x^{p^{3n}} y^{p^{2n}} z) L_4^{p^n-1} + (x^{p^{4n}} y^{p^{3n}} z^{p^{2n}})}{(x^{p^{3n}} y^{p^{2n}} z^{p^n})},$$

which will be identified with Q_{42} and Q_{41}, respectively.

6. For general m, we obtain the desired expressions for Q_{ms} by means of the following determinant, which vanishes identically:

$$D_s = \begin{vmatrix} A & A' \\ O & B \end{vmatrix},$$

where O is a matrix of $m-2$ rows and m columns all of whose elements are zero, A' is derived from A by deleting the last column, and *

$$A = \begin{vmatrix} x_1^{p^{nm}} & \cdots & x_m^{p^{nm}} \\ x_1^{p^{n(m-1)}} & \cdots & x_m^{p^{n(m-1)}} \\ \cdots & \cdots & \cdots \\ x_1^{p^n} & \cdots & x_m^{p^n} \\ x_1 & \cdots & x_m \end{vmatrix}, \qquad B = \begin{vmatrix} x_1^{p^{n(m-1)}} & \cdots & x_{m-1}^{p^{n(m-1)}} \\ \cdots & \cdots & \cdots \\ x_1^{p^{n(s+1)}} & \cdots & x_{m-1}^{p^{n(s+1)}} \\ x_1^{p^{n(s-1)}} & \cdots & x_{m-1}^{p^{n(s-1)}} \\ \cdots & \cdots & \cdots \\ x_1^{p^n} & \cdots & x_{m-1}^{p^n} \end{vmatrix}.$$

By Laplace's development of D_s we get

$$\begin{aligned} &(-1)^{m-2}[m, \cdots, 1][m-1, \cdots, s+1, s-1, \cdots, 1, 0] \\ &\quad + (-1)^s (-1)^{m-s-1}[m, \cdots, s+1, s-1, \cdots, 0][m-1, \cdots, 1] \\ &\quad + (-1)^m [m-1, \cdots, 0][m, \cdots, s+1, s-1, \cdots, 1] = 0. \end{aligned}$$

* If $s = 1$, the exponents in the last row of B are p^{2n}; if $s = m-1$, the exponents in the first row are $p^{n(m-2)}$.

Let the factor $(-1)^m$ be removed. For $1 < s < m-1$, we get

$$L_m^{p^m} \cdot Q_{m-1,s} L_{m-1} - Q_{ms} L_m \cdot L_{m-1}^{p^m} + L_m (Q_{m-1\,s-1} L_{m-1})^{p^m} = 0,$$

$$Q_{ms} = Q_{m-1\,s} \left(\frac{L_m}{L_{m-1}} \right)^{p^m-1} + Q_{m-1\,s-1}^{p^m} \qquad (1 < s < m-1). \tag{4}$$

For $s = 1$ and $s = m-1$, we obtain respectively

$$L_m^{p^m} \cdot Q_{m-1\,1} L_{m-1} - Q_{m1} L_m \cdot L_{m-1}^{p^m} + L_m \cdot L_{m-1}^{p^{2m}} = 0,$$

$$L_m^{p^m} \cdot L_{m-1} - Q_{m\,m-1} L_m \cdot L_{m-1}^{p^m} + L_m (Q_{m-1\,m-2} L_{m-1})^{p^m} = 0,$$

$$Q_{m1} = Q_{m-1\,1} \left(\frac{L_m}{L_{m-1}} \right)^{p^m-1} + L_{m-1}^{p^{2m}-p^m}, \qquad Q_{m\,m-1} = \left(\frac{L_m}{L_{m-1}} \right)^{p^m-1} + Q_{m-1\,m-2}^{p^m}. \tag{5}$$

As a check, we observe that the terms free of x_m, namely the final terms in (4) and (5), equal the quotient of the coefficients of z in the numerator and denominator of Q_{mi}. We note that

$$p^{nm} - p^{ns} = \text{degree of } Q_{ms}, \qquad p^{n(m-1)} + \cdots + p^n + 1 = \text{degree of } L_m. \tag{6}$$

Expanding L_m according to the last column and introducing the Q_{ms} of § 1, we get

$$L_m = x_m L_{m-1}^{p^m} + L_{m-1} \sum_{s=1}^{m-2} (-1)^s x_m^{p^{ms}} Q_{m-1,s} + (-1)^{m-1} x_m^{p^{m(m-1)}} L_{m-1}. \tag{7}$$

Hence (4) and (5) may be given an integral form.

Fundamental System of Invariants of G_m.

7. **Theorem.** *The functions L_μ, $Q_{\mu 1}, \cdots, Q_{\mu\,\mu-1}$ are independent and form a fundamental system of invariants for G_μ.*

We assume that the theorem is true for $\mu \leqq m$, where $m \geqq 2$, and prove that it is true for $\mu = m+1$.

Let I be any homogeneous integral invariant of G_{m+1}. The coefficients of the various powers of x_{m+1} in I are invariants of G_m and hence by hypothesis are integral functions of L_m, $Q_{m1}, \cdots, Q_{m\,m-1}$. In particular, the sum I_0 of the terms of I free of x_{m+1} is an aggregate of terms

$$t' = c' L_m^{a'} Q_{m1}^{b'_1} \cdots Q_{m\,m-1}^{b'_{m-1}} \qquad (c' \neq 0).$$

Consider the set of terms t' in which a' has the minimum value a, the subset in which b'_1 has the minimum value b_1, etc. In the resulting unique term

$$t = c L_m^a Q_{m1}^{b_1} \cdots Q_{m\,m-1}^{b_{m-1}},$$

the term of minimum degree in x_m is, by (4), (5), (7), $x_m^{a_1} t_1$, where

$$t_1 = c L_{m-1}^{a_1} \prod_{s=2}^{m-1} Q_{m-1\,s-1}^{p^m b_s} \qquad (a_1 = ap^n + b_1 d).$$

Similarly, the term of t_1 of minimum degree in x_{m-1} is $x_{m-1}^{a_1} t_2$,

$$t_2 = cL_{m-2}^{a_1} \prod_{s=3}^{m-1} Q_{m-2\,s-2}^{p^{a_s} b_s} \qquad (a_2 = a_1 p^n + p^n b_2 d).$$

Proceeding in this manner, we see that t contains a term

$$\tau = cx_m^{a_0} x_{m-1}^{a_1} x_{m-2}^{a_2} \cdots x_{m-i}^{a_i} \cdots x_1^{a_{m-1}} \quad (a_i = a_{i-1} p^n + p^{n(i-1)} b_i d),$$

where $a_0 = a$. Evidently τ occurs but once in the product t. Further, τ does not occur in a product t' distinct from t. For, if so, $a' = a$ and hence (by a_1) $b_1' = b_1$, then (by a_2) $b_2' = b_2$, etc., so that $t' \equiv t$. Hence I has the isolated term τ and therefore also

$$x_{m+1}^{a_1} \tau_1, \qquad \tau_1 \equiv c x_{m-1}^{a_1} x_{m-2}^{a_2} \cdots x_1^{a_{m-1}}.$$

Hence τ_1 is a term of an invariant of G_m. The latter invariant has the term

$$x_m^{a_2} \tau_2, \qquad \tau_2 \equiv c x_{m-2}^{a_2} x_{m-3}^{a_3} \cdots x_1^{a_{m-1}}.$$

Hence τ_2 is a term of an invariant of G_{m-1}. Proceeding in this manner, we see that $\tau_m = cx_1^a$ is a term of an invariant of G_2. Hence cx_1^a is a term of kQ_{21}^{α}, whence $a = \alpha d$.

By (6_1) the degree of Q_{ms} is a multiple of p^n. Since a is a multiple of p^n, it follows that t is of degree a multiple of p^n. Since this is therefore true of t, and since the degree of L_m is prime to p, by (6_2), it follows that a' is a multiple of p^n. As in § 3, a' is a multiple of $p^n - 1$. Hence *in every term t' of I_0, a' is a multiple of $d = p^n(p^n - 1)$.*

By (4), (5), (7), we have

$$Q_{m1} = L_{m-1}^d + x_m^r L_{m-1}^{r^2} Q_{m-1\,1} + \cdots, \qquad Q_{ms} = Q_{m-1\,s-1}^{p^n} + x_m^r L_{m-1}^{r^2} Q_{m-1\,s} + \cdots \quad (s > 1),$$

the final Q being suppressed if $s = m - 1$. In these series the exponents of x_m differ by multiples of $r = p^n - 1$. Let $b_s = p^{\beta_s} B_s$, where B_s is prime to p. To obtain the power p^β of a sum in a field having modulus p, we have only to multiply every exponent by p^β. Hence we get

$$(8) \qquad L_m^a = (L_m^{p^n})^{ar} = x_m^a L_{m-1}^{ap^n} - \alpha r x_m^{a+d} L_{m-1}^{ap^n - d} Q_{m-1\,1}^{p^n} + \cdots,$$

$$(9) \qquad Q_{m1}^{b_1} = L_{m-1}^{db_1} + B_1 x_m^{rp^{\beta_1}} L_{m-1}^{e} Q_{m-1\,1}^{p^{\beta_1}} + \cdots \qquad (e = db_1 - rp^{\beta_1}),$$

$$(10) \qquad Q_{ms}^{b_s} = Q_{m-1\,s-1}^{p^n b_s} + B_s x_m^{rp^{\beta_s}} L_{m-1}^{r^2 p^{\beta_s}} Q_{m-1\,s-1}^{e_s} Q_{m-1\,s}^{p^{\beta_s}} + \cdots \quad (e_s = b_s p^n - p^{n+\beta_s}),$$

where in the last series $s > 1$ and the term $Q_{m-1\,s}$ is to be suppressed if $s = m - 1$. Hence t/c contains the terms

$$T_1 = B_1 x_m^{a + rp^{\beta_1}} L_{m-1}^{e + ap^n} Q_{m-1\,1}^{p^{\beta_1}} \prod_{s=2}^{m-1} Q_{m-1\,s-1}^{p^n \beta_s},$$

$$T_\sigma = B_\sigma x_m^{a + rp^{\beta_\sigma}} L_{m-1}^{h_\sigma} Q_{m-1\,\sigma-1}^{e_\sigma} Q_{m-1\,\sigma}^{p^{\beta_\sigma}} \prod Q_{m-1\,s-1}^{p^n b_s} \qquad (h_\sigma = ap^n + db_1 + r^2 p^{\beta_\sigma}),$$

where $\sigma > 1$ and $Q_{m-1\,\sigma}$ is to be suppressed if $\sigma = m-1$, and where in the final product s has the values $2, \cdots, \sigma-1, \sigma+1, \cdots, m-1$.

First, let $\beta_1 < n$. Then $rp^{\beta_1} < d$. The product t contains but one term with the same set of exponents as T_1. For, if we employ a term of (9) after the second, the exponent of x_m exceeds that in T_1; if we employ the second term in (9), we must use the first terms in (8) and (10) and hence get T_1 itself; if we employ the first term of (9), we must use the first term of (8), and obtain as the exponent of L_{m-1} in the product of the two

$$ap^n + db_1 > e + ap^n.$$

Suppose that T_1 is a term of a product t' distinct from t. If $a' > a$, then $a' \geqq a + d$, since a' and a are multiples of d. Thus the minimum exponent a' of x_m in t' would exceed the exponent of x_m in T_1. Hence $a' = a$. Hence by (6) and the homogeneity of our invariant,

$$\sum_{s=1}^{m-1} (b_s' - b_s)(p^{nm} - p^{ns}) = 0. \tag{11}$$

Hence $(b_1' - b_1)p^n$ is a multiple of p^{2n}, so that

$$b_1' \equiv a_1 \pmod{p^n} \qquad \text{when} \qquad a' = a. \tag{12}$$

Thus in $b_1' = p^{\beta_1'} B_1'$, we have $\beta_1' = \beta_1$. Hence T_1 cannot occur in terms of t' other than

$$x_m^a L_{m-1}^{ap^n} (L_{m-1}^{db_1'} + B_1' x_m^{rp^{\beta_1}} L_{m-1}^{c'} Q_{m-1\,1}^{p^{\beta_1}}) \prod_{s=2}^{m-1} Q_{ms}^{b_s'}. \tag{13}$$

If we employ the second term in the parenthesis, we must take the term of each Q_{ms} free of x_m. Then $b_1' = b_1$, from the exponents of L_{m-1}, and $b_s' = b_s$ $(s = 2, \cdots, m-1)$, from the exponents of $Q_{m-1\,s-1}$. But $t' \neq t$. If we employ the first term in the parenthesis in (13), we obtain as the exponent of L_{m-1} in the product of the first two factors

$$ap^n + db_1' > e + ap^n,$$

since $b_1' \geqq b_1$ when $a' = a$. Hence the assumption is false.

We have now shown that T_1 occurs as an isolated term of the invariant. But the exponent of x_m is not a multiple of d and the coefficient B_1 is not zero in the field. Hence this case $\beta < n$ is excluded. Thus b_1 is a multiple of p^n.

Of the numbers $b_1, \cdots, b_{m-1}$ not multiples of p^n, let b_σ be the one with smallest subscript. Then $\sigma > 1$. A term of t with the same set of exponents as T_σ can be obtained only by taking the first terms of (8), (9), (10), for $s < \sigma$. If we use the second term of (10) for $s = \sigma$, we must take the first term of (10) for $s > \sigma$ and then obtain T_σ. If we use the first term of (10) for $s = \sigma$, the exponent of $Q_{m-1\,\sigma-1}$ in the product is $p^n b_\sigma$, which exceeds its exponent e_σ in T_σ.

Next, if T_σ occurs in t', distinct from t, then $a' = a$. From (12) it now follows that b_1' is a multiple of p^n. Analogous to (9),

$$Q_{m1}^{b_1'} = L_{m-1}^{db_1'} + x_m^{d'} K. \tag{14}$$

Hence we must take the first terms of (8) and (14). In the product of these two, the exponent of L_{m-1} is $ap^n + db_1' > h_\sigma$ if $b_1' \geqq b_1 + p^n$. Hence* must $b_1' = b_1$. If $\sigma > 2$, b_2 is by hypothesis a multiple of p^n. Then by (11), b_2' is a multiple of p^n. Hence we must take the first term $Q_{m-1\,1}^{p^n b_2'}$ of $Q_{m2}^{b_2'}$. Since $Q_{m-1\,1}$ does not occur in the expansion of Q_{ms} for $s > 2$, and occurs in T_σ with the exponent $p^n b_2$, we conclude that $b_2' = b_2$. In this manner we may show that we must take the first term of $Q_{ms}^{b_s'}$ $(s < \sigma)$ and that $b_s' = b_s$ $(s = 2, \cdots, \sigma - 1)$. Then by (11), $b_\sigma' \equiv b_\sigma \pmod{p^n}$, whence $\beta_\sigma' = \beta_\sigma$. If we employ the second term in $Q_{m\sigma}^{b_\sigma'}$, we must use the first term in $Q_{ms}^{b_s'}$ $(s > \sigma)$ and we obtain the term T_σ if and only if $b_s' = b_s$ $(s = \sigma, \cdots, m-1)$, as shown by comparing the exponents of Q_{m-1s} $(s \geqq \sigma)$. But then $t' \equiv t$. If we employ the first term in $Q_{m\sigma}^{b_\sigma'}$, the total exponent of $Q_{m-1\sigma-1}$ in t' is $p^n b_\sigma'$ which exceeds its exponent e_σ in T_σ since $b_\sigma' \geqq b_\sigma$, in view of our definition of t.

We have now shown that τ_σ occurs as an isolated term of the invariant. But the exponent of x_m is not a multiple of d and the coefficient B_σ is not zero in the field. Hence our assumption on b_σ is false, so that $b_1, \cdots, b_{m-1}$ are all multiples of p^n. Set $b_s = p^n c_s$. Then

$$I' = I - c Q_{m+1\,1}^{\sigma} \prod_{s=1}^{m-1} Q_{m+1\,s+1}^{c_s}$$

is an invariant of G_{m+1} in which I_0' lacks t. As at the end of § 3, it follows that I is an integral function of L_{m+1}, Q_{m+1i} $(i = 1, \cdots, m)$.

It remains to prove that the latter invariants are independent.† Any rational integral relation between them can be given the form

$$A L_{m+1} + B(Q_{m+11}, \cdots, Q_{m+1m}) = 0.$$

Let $x_{m+1} = 0$. Then by (4) and (5) with m replaced by $m+1$, we get

$$B(L_m^d, Q_{m1}^{p^n}, \cdots, Q_{mm-1}^{p^n}) = 0.$$

But L_m and the Q_{ms} are independent by hypothesis. Hence $B \equiv 0$. Thus the initial relation has the factor L_{m+1}. Since the relation cannot reduce to $L_{m+1}^\lambda \equiv 0$, it may be given the form $A' L_{m+1} + B' = 0$. As before $B' \equiv 0$. A repetition of this argument shows that no relation exists between the L_{m+1}, Q_{m+1i}.

As a basis for our induction, we note that there is no relation $A L_2 + c Q_{21}^{\gamma} = 0$

* For $m = 3$, (11) gives $b_2' = b_2$, whence $t' \equiv t$.

† Another proof follows from the existence of solutions of the form problem (§ 8), whatever values be assigned to the fundamental invariants.

between the invariants of G_2. For, by setting $y = 0$, we get $cx^{p^4} = 0$, whence $c = 0$. Proceeding similarly with $A = A'L_2 + c'Q_{21}^{r'} = 0$, we prove that $A \equiv 0$.

The Form Problem.

8. In discussing the solution of a set of equations with coefficients in a finite field having modulus p, it is convenient to introduce the infinite field F_p composed of all the roots of all rational integral equations with integral coefficients taken modulo p. Then F_p, like the field of all complex numbers, has the property that any algebraic equation of degree k with coefficients in the field has k roots in the field.

In the form problem for the group G_m, we seek the sets of values of the m variables x_i for which the m fundamental absolute invariants L_m^r, Q_{ms} $(s = 1, \cdots, m-1)$ take assigned values λ, q_s in F_p. Here $r = p^n - 1$. If l is a particular r-th root of λ, the problem * consists in the solution of

$$L_m(x_i) = l, \qquad Q_{ms}(x_i) = q_s \qquad (s = 1, \cdots, m-1). \tag{15}$$

Let $x_1, \cdots, x_m$ be a set of solutions of (15). Since the determinant L_{m+1} vanishes when x_{m+1} equals one of the x_i $(i \leqq m)$, it follows from (7), with m replaced by $m+1$, that $x_1, \cdots, x_m$ are roots of

$$l\xi^{p^{nm}} + \sum_{s=1}^{m-1} (-1)^{m-s} l q_s \xi^{p^{ns}} + (-1)^m l^{p^n} \xi = 0. \tag{16}$$

Suppose for the present that $l \neq 0$. The preceding equation gives

$$\xi^{p^{nm}} + \sum_{s=1}^{m-1} (-1)^{m-s} q_s \xi^{p^{ns}} + (-1)^m \lambda \xi = 0. \tag{17}$$

This equation has no double root and hence has p^{nm} distinct roots in F_p. If ξ_1 and ξ_2 are roots, then are also $\xi_1 + \xi_2$, $c_1\xi_1$, where c_1 is an element of the $GF[p^n]$. Indeed, in that field,

$$(\xi_1 + \xi_2)^{p^{ns}} = \xi_1^{p^{ns}} + \xi_2^{p^{ns}}, \qquad (c_1\xi_1)^{p^{ns}} = c_1\xi_1^{p^{ns}}.$$

Hence there exist m solutions $\xi_1, \cdots, \xi_m$ of (17), linearly independent with respect to the $GF[p^n]$, while ξ is a solution if and only if

$$\xi = c_1\xi_1 + \cdots + c_m\xi_m \qquad (c\text{'s in } GF[p^n]). \tag{18}$$

Since the x_i are solutions, we have

$$x_i = c_{i1}\xi_1 + \cdots + c_{im}\xi_m \qquad (i = 1, \cdots, m), \tag{19}$$

in which the c_{ij} are elements of non-vanishing determinant of the $GF[p^n]$. Indeed, by § 1,

$$l = L_m(x_i) = |c_{ij}| \cdot L_m(\xi_i). \tag{20}$$

* This problem is the form problem for the subgroup G_m' of all the transformations of determinant unity.

To show conversely that any such set of values (19) satisfy equations (15), let $\xi_1, \cdots, \xi_m$ be any set of roots of (17) linearly independent with respect to the $GF[p^n]$. Then by § 2, $L_m(\xi_i) \neq 0$. Define the x_i by (19), where $|c_{ij}| \neq 0$. Then $l \neq 0$ by (20). By § 2, the p^{nm} expressions (18) are the roots of

$$L_{m+1}(\xi_1, \cdots, \xi_m, \xi) = 0,$$

in which the coefficient of $\xi^{p^{nm}}$ is $\pm L_m(\xi_i) \neq 0$, and hence are the roots of

$$\xi^{p^{nm}} + \sum_{s=1}^{m-1} (-1)^{m-s} Q_{ms}(\xi_i) \xi^{p^{ns}} + (-1)^m [L_m(\xi_i)]^r \xi = 0.$$

Since this equation and (17) have in common the p^{nm} distinct roots (18), they are identical. In view of the absolute invariance of L_m^r and Q_{ms}, we conclude that the expressions (19) satisfy equations (15), in which $l^r = \lambda$.

Theorem. *For $\lambda \neq 0$, $x_1, \cdots, x_m$ is a set of solutions of*

$$L_m^{p^n-1} = \lambda, \qquad Q_{ms} = q_s \qquad (s = 1, \cdots, m-1) \tag{21}$$

if and only if $x_i = c_{i1}\xi_1 + \cdots + c_{im}\xi_m$ $(i = 1, \cdots, m)$, where the c_{ij} are elements of non-vanishing determinant of the $GF[p^n]$, and $\xi_1, \cdots, \xi_m$ is any set of roots of equation (17) *linearly independent with respect to the $GF[p^n]$.*

To obtain the sets of solutions of (15), we restrict the c_{ij} to be of determinant unity and hence, by (20), the ξ_i to be linearly independent roots of (17) for which $L_m(\xi_i) = l$.

Next, let $\lambda = 0$, $q_1 \neq 0$. If the minors of the elements of the first row of L_m all vanished, there would exist (§ 2) a linear relation between each set of $m-1$ of the x's. Applying a linear transformation, we would obtain $x_m = x_{m-1} = 0$. By (7) the quotient L_m/L_{m-1} would vanish and, by (5_1), $Q_{m1} = 0$, in contradiction with $q_1 \neq 0$. Hence the above minors are not all zero. After permuting the variables we may set $L_{m-1} \neq 0$. Then, by (4) and (5),

$$L_{m-1}^{p^n(p^n-1)} = q_1, \qquad Q_{m-1\,s-1}^{p^n} = q_s \qquad (s = 2, \cdots, m-1).$$

As above, $x_1, \cdots, x_{m-1}$ are linear functions of a set of linearly independent roots $\xi_1, \cdots, \xi_{m-1}$ of

$$\xi^{p^{n(m-1)}} + \sum_{\sigma=2}^{m-1} (-1)^{m-\sigma} q_\sigma^{1/p^n} \xi^{p^{n(\sigma-1)}} + (-1)^{m-1} q_1^{1/p^n} \xi = 0,$$

given by (7) upon replacing s by $\sigma - 1$. Raising this equation to the power p^n we obtain (17) for $\lambda = 0$. Each root of the latter is therefore of multiplicity exactly p^n. In view of $L_m = 0$, there exists (§ 2) a linear relation between $x_1, \cdots, x_m$, with coefficients in the $GF[p^n]$. Since $x_1, \cdots, x_{m-1}$ are linearly independent with respect to this field, x_m is a linear function of $x_1, \cdots, x_{m-1}$ and hence of $\xi_1, \cdots, \xi_{m-1}$, with coefficients in this field. Returning to the initial order of the variables, we conclude that, if $\lambda = 0$, $q_1 \neq 0$, $x_1, \cdots, x_m$ are

linear functions of a set $m-1$ linearly independent roots of (17), the matrix of the coefficients being of rank $m-1$.

Next, let $\lambda = q_1 = 0$, $q_2 \neq 0$. Then the minors of the elements of the first row of L_m all vanish. For, if $L_{m-1} \neq 0$, for example, (5_1) would give $Q_{m1} \neq 0$, contrary to $q_1 = 0$. After applying a linear transformation T, we may set $x_m = x_{m-1} = 0$. Then by (7) the quotient L_m/L_{m-1} is zero. Hence by (4) and (5_2),

$$Q^{p^n}_{m-1\,s-1} = q_s \qquad (s = 2, \cdots, m-1).$$

By (7), with m replaced by $m-1$, the quotient L_{m-1}/L_{m-2} vanishes when $x_{m-1} = 0$. Hence by (4) and (5), with m replaced by $m-1$,

$$L^{p^{2n}(p^n-1)}_{m-2} = q_2, \qquad Q^{p^{2n}}_{m-2\,s-2} = q_s \qquad (s = 3, \cdots, m-1).$$

If, for $i \leqq m-2$, we multiply the elements of the i-th column of L_{m-1} by the adjoint minors of the corresponding elements of the last column, we see (compare (7) with m replaced by $m-1$) that $x_1, \cdots, x_{m-2}$ are roots of

$$0 = \xi L^{p^n}_{m-2} + L_{m-2} \sum_{s=1}^{m-3} (-1)^s \xi^{p^{ns}} Q_{m-2\,s} + (-1)^{m-2} \xi^{p^{n(m-2)}} L_{m-2}.$$

Divide by L_{m-2} and raise the resulting equation to the power p^{2n}. We obtain equation (17), since $\lambda = q_1 = 0$. Each root of the latter is now of multiplicity p^{2n}. As above, $x_1, \cdots, x_{m-2}$ are linearly independent linear functions of $m-2$ linearly independent roots $\xi_1, \cdots, \xi_{m-2}$ of (17). Applying the inverse of T, we conclude that the initial values $x_1, \cdots, x_m$ are linear functions of $\xi_1, \cdots, \xi_{m-2}$, the matrix of the coefficients being of rank $m-2$.

Proceeding in a similar manner, we obtain the

Theorem. *If $\lambda = q_1 = \cdots = q_{t-1} = 0$, $q_t \neq 0$, then $x_1, \cdots, x_m$ is a set of solutions of (21) if and only if the x_i are linear functions of $\xi_1, \cdots, \xi_{m-t}$ with coefficients in the $GF[p^n]$ the rank of whose matrix is $m-t$, while $\xi_1, \cdots, \xi_{m-t}$ is any set of roots of (17) linearly independent with respect to the $GF[p^n]$, every root of (17) being a linear function of these $m-t$ roots. If all the invariants are zero, each x_i is zero.*

9. The number of matrices (c_{ij}) of rank $m-t$ with m rows and $m-t$ columns, each c_{ij} being an element of the $GF[p^n]$, is

$$(22) \qquad (p^{nm}-1)(p^{nm}-p^n)\cdots(p^{nm}-p^{n(m-t-1)}).$$

Hence this gives the number of distinct sets of solutions of the form problem when $\lambda = q_1 = \cdots = q_{t-1} = 0$, $q_t \neq 0$.

From the above discussion follows the

Theorem. *The determinant L_m is of rank $m-t$ if and only if*

$$(23) \qquad L_m = 0, \quad Q_{m1} = 0, \quad \cdots, \quad Q_{m\,t-1} = 0, \quad Q_{mt} \neq 0.$$

These are necessary and sufficient invariantive conditions that the variables x_i shall satisfy exactly t linearly independent linear relations in the $GF[p^n]$.

Solution of the Fundamental Equation.

10. The complete solution of the form problem has been reduced to the solution of the fundamental equation (17). If $\lambda = 0$, the latter equation is the p^n-th power of an equation of like type. Hence it suffices to discuss the solution of equations of type (17) with $\lambda \neq 0$.

We may restrict attention to the case in which the coefficients of (17) belong to the $GF[p^n]$, since in the contrary case the equation is equivalent to one of like form with coefficients in the $GF[p^n]$, but of higher degree. The nature of the proof will be indicated for $m = 2$. Then (17) becomes

$$\xi^{p^{2n}} = q\xi^{p^n} - \lambda\xi. \tag{24}$$

Let q be a root of an equation $Q^2 - aQ + b = 0$, irreducible in the $GF[p^n]$. Its second root is q^{p^n}, so that

$$q^{p^n} + q = a, \qquad q^{p^n+1} = b, \qquad q^{p^{2n}} = q.$$

From the p^n-th power of (24) we eliminate $\xi^{p^{2n}}$ and get

$$\xi^{p^{3n}} = (b - \lambda^{p^n})\xi^{p^n} - q^{p^n}\lambda\xi.$$

From the p^n-th power of the latter we eliminate $q\xi^{p^n}$ by (24) and get

$$\xi^{p^{4n}} = \beta\xi^{p^{2n}} - \lambda^{p^n+1}\xi, \qquad \beta = b - \lambda^{p^{2n}} - \lambda^{p^n}. \tag{25}$$

If λ belongs to the $GF[p^n]$, the required equation is thus

$$\xi^{p^{4n}} - (b - 2\lambda)\xi^{p^{2n}} + \lambda^2\xi = 0. \tag{26}$$

If λ is a root of an equation $L^2 - rL + s = 0$, irreducible in the $GF[p^n]$, the required equation is obviously

$$\xi^{p^{4n}} - (b - r)\xi^{p^{2n}} + s\xi = 0. \tag{27}$$

If λ is a root of an equation $\lambda^3 - c\lambda^2 + d\lambda - e = 0$, irreducible in the $GF[p^n]$, we make repeated use of the relations

$$\lambda + \lambda^{p^n} + \lambda^{p^{2n}} = c, \qquad \lambda^{1+p^n+p^{2n}} = e,$$

raise (25) to the powers $p^{2n}, p^{4n}, \cdots, p^{8n}$, and find that

$$\xi^{p^{12n}} - \{b(b-c)^2 - 2e\}\xi^{p^{6n}} + e^2\xi = 0. \tag{28}$$

11. We therefore consider the fundamental equation (17) with coefficients in the $GF[p^n]$ and $\lambda \neq 0$. There is no multiple root. Let r be a root $\neq 0$.

If $r^{p^n} = xr$, where x belongs to the $GF[p^n]$ then

$$r^{p^{2n}} = xr^{p^n} = x^2 r, \qquad r^{p^{jn}} = x^j r.$$

Hence, by (17), x must satisfy the *characteristic equation*

$$\Delta(x) \equiv x^m + \sum_{s=1}^{m-1} (-1)^{m-s} q_s x^s + (-1)^m \lambda = 0. \tag{29}$$

Thus each root in the $GF[p^n]$ of $\Delta(x) = 0$ furnishes a factor $\xi^{p^n} - x\xi$ of (17). Let this binomial have a factor $f(\xi)$, of degree d, irreducible in the $GF[p^n]$. Its roots are

$$r, \ r^{p^n} = xr, \ r^{p^{2n}} = x^2 r, \ \cdots, \ r^{p^{(d-1)n}} = x^{d-1} r,$$

while x belongs to the exponent d. Since x is in the field, d is a divisor of $p^n - 1$. It follows that

$$f(\xi) = \xi^d - \delta \qquad (\delta = r^d).$$

Theorem. *The irreducible factors of $\xi^{p^n-1} - x$ are all binomial and of equal degree, namely, the exponent to which x belongs.*

Discussion of the Fundamental Equation for $m = 2$.

12. For the present, let $m = 2$. Since $2p^n - 1 < p^{2n}$, equation (24) has an irreducible factor $F(\xi)$, of degree $D > 1$, not of the preceding type $f(\xi)$, and hence has a root r such that r^{p^n}/r is not an element of the $GF[p^n]$. Since, therefore, r and r^{p^n} are linearly independent with respect to that field, we conclude from (18) that every root of (24) is of the form $c_1 r + c_2 r^{p^n}$, where c_1 and c_2 are elements of the $GF[p^n]$. Hence (24) has all its roots in the $GF[p^{nD}]$, but not all in a smaller field.

Theorem. *For $m = 2$, every irreducible factor of the fundamental equation is of degree a divisor of D; each irreducible factor not of the above binomial type is of degree D.*

13. We proceed to determine this integer D which is such that equation (24) is completely solvable in the $GF[p^{nD}]$, but not in the $GF[p^{nl}]$, for $l < D$. By raising (24) to the powers $p^n, p^{2n}, \cdots$, we may express $\xi^{p^{nt}}$ as a linear function l_t of ξ^{p^n} and ξ. We seek the least value D of t for which $l_t \equiv \xi$. Now the coefficients of l_t are the elements of the first line in S^{t-1}, where

$$S = \begin{pmatrix} q & -\lambda \\ 1 & 0 \end{pmatrix}, \qquad \Delta(x) = x^2 - qx + \lambda.$$

The condition for $l_{D+1} = \xi^{p^n}$ is therefore $S^D = 1$. Hence D is the period of the transformation S. According as the characteristic equation $\Delta(x) = 0$ has distinct roots x_1 and x_2 or equal* roots $x = \frac{1}{2}q = \lambda^{\frac{1}{2}}$, the canonical form for S is

$$\begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}, \qquad \begin{pmatrix} x & x \\ 0 & x \end{pmatrix}.$$

In the first case, the period of S is the least common multiple of the exponents

* We then employ the new variables $V_1 = v_1$, $V_2 = v_1 - xv_2$.

to which the roots x_1 and x_2 belong. In the second case, the period is p times the exponent to which the double root belongs.

Theorem. *For $m = 2$, the fundamental equation is completely solvable in the $GF[p^{nD}]$, but in no lower field, where D is the least common multiple of the exponents to which belong distinct roots of the characteristic equation, or p times the exponent to which its double root belongs.*

Illustrations of the preceding results are afforded by the following examples in which are given all the irreducible factors other than ξ of (24):

$p^n = 2$. $\xi^3 + 1 \equiv (\xi + 1)(\xi^2 + \xi + 1)$, $\xi^3 - \xi + 1$ irreducible;

$p^n = 3$. $\xi^8 - 1 \equiv (\xi + 1)(\xi - 1)(\xi^2 + 1)(\xi^2 + \xi - 1)(\xi^2 - \xi - 1)$,

$\xi^8 \pm \xi^2 - 1$ irreducible, $\xi^8 + \xi^2 + 1 \equiv (\xi+1)(\xi-1)(\xi^3-\xi+1)(\xi^3-\xi-1)$,

$\xi^8 + 1 \equiv (\xi^4+\xi^2-1)(\xi^4-\xi^2-1)$, $\xi^8 - \xi^2 + 1 \equiv (\xi^2+1)(\xi^6 - \xi^4 + \xi^2 + 1)$.

Theory of the General Fundamental Equation.

14. We remove the restriction that $m = 2$ and prove the

Theorem. *If the characteristic function* (29) *reduces in the $GF[p^n]$,*

$$(30)\quad \Delta(x) = \phi(x)\psi(x), \quad \phi(x) = \sum_{i=0}^{\alpha} a_i x^i, \quad \psi(x) = \sum_{j=0}^{m-\alpha} b_j x^j, \quad a_\alpha = b_{m-\alpha} = 1,$$

the fundamental equation (17) *is transformed into*

$$(31)\qquad \Psi(\eta) \equiv \sum_{j=0}^{m-\alpha} b_j \eta^{p^{nj}} = 0$$

by the substitution

$$(32)\qquad \eta = \Phi(\xi) \equiv \sum_{i=0}^{\alpha} a_i \xi^{p^{ni}}.$$

In other words, the fundamental equation factors into*

$$\prod_{k=1}^{p^{n(m-\alpha)}} [\Phi(\xi) - \eta_k] = 0 \qquad [\eta_k \text{ roots of } \Psi(\eta) = 0].$$

For proof, we note that the result of the elimination of η is

$$\sum a_i b_j \xi^{p^{n(i+j)}} \qquad (i = 0, \cdots, \alpha;\ j = 0, \cdots, m-\alpha),$$

which is identical with (17), since by (30) the corresponding sum $\sum a_i b_j x^{i+j}$ is identical with (29).

Since equation (31) has the root $\eta = 0$, we obtain

Corollary I. The fundamental equation has the factor $\Phi(\xi)$ if and only if the characteristic equation has the factor $\phi(x)$ in the $GF[p^n]$.

Corollary II. A root of the fundamental equation satisfies $\Phi(\xi) = 0$, but no similar equation of lower degree, if and only if $\phi(x)$ is a factor of $\Delta(x)$.

* Hence it has the symbolic expression $\psi(\phi)$, as in the theory of the reducibility of linear differential equations.

15. For $k \leqq m$ let D_k denote the number of the non-vanishing roots of the fundamental equation each of which satisfies an equation $\Phi_k(\xi) = 0$, but no equation $\Phi_l(\xi) = 0$, $l < k$. By corollary II, $\phi_k(x)$ must be a factor of $\Delta(x)$. Suppose first that the latter has no multiple factors. Denote by $N_1, N_2, N_3, \cdots$ the number of its irreducible factors of degree $1, 2, 3, \cdots$. Then

$$m = N_1 + 2N_2 + 3N_3 + \cdots.$$

Let $[i] = p^{ni} - 1$. We proceed to show that

$$D_k = \Sigma \binom{N_1}{n_1}\binom{N_2}{n_2}\cdots\binom{N_k}{n_k}[1]^{n_1}[2]^{n_2}\cdots[k]^{n_k}, \tag{33}$$

the sum extending over all sets of positive integers n_i for which

$$k = n_1 + 2n_2 + 3n_3 + \cdots + kn_k, \qquad n_i \leqq N_i.$$

Let a particular factor ϕ_k of $\Delta(x)$ contain $n_1, n_2, n_3, \cdots$ irreducible factors of degree $1, 2, 3, \cdots$. Of the $[k]$ roots of the corresponding equation $\Phi_k(\xi) = 0$, we wish to exclude those which satisfy $\Phi_l(\xi) = 0$, $l < k$. Let ϕ_l have $m_1, m_2, m_3, \cdots$ irreducible factors of degree $1, 2, 3, \cdots$. We assume that (33) holds when k is replaced by a smaller value l. Then the number of roots to be excluded is

$$E = \sum_{l=1}^{k-1} \Sigma \binom{n_1}{m_1}\binom{n_2}{m_2}\cdots\binom{n_l}{m_l}[1]^{m_1}[2]^{m_2}\cdots[l]^{m_l},$$

the inner sum extending over all sets of positive integers m_i for which

$$l = m_1 + 2m_2 + \cdots + lm_l, \qquad m_i \leqq n_i.$$

To prove (33), it remains to show that

$$[k] - E = [1]^{n_1}[2]^{n_2}\cdots[k]^{n_k}.$$

This follows from *

$$1 + E + [1]^{n_1}\cdots[k]^{n_k} = \sum_{l=0}^{k} \Sigma \binom{n_1}{m_1}\cdots\binom{n_l}{m_l}[1]^{m_1}\cdots[l]^{m_l}$$

$$= \left\{\sum_{m_1=0}^{n_1}\binom{n_1}{m_1}[1]^{m_1}\right\}\cdots\left\{\sum_{m_k=0}^{n_k}\binom{n_k}{m_k}[k]^{m_k}\right\} = \{1+[1]\}^{n_1}\cdots\{1+[k]\}^{n_k} = p^{nk}.$$

Hence if $\Delta(x)$ has no multiple root, the number of the roots of the fundamental equation which satisfy no similar equation of lower degree is

$$D_m = [1]^{N_1}[2]^{N_2}\cdots[m]^{N_m}.$$

If the characteristic equation has multiple roots,

$$\Delta(x) = \prod_i F_{d_i}^{e_i},$$

* Note that, for the added term, $l = k$, whence $m_i = n_i$.

where the F's are distinct irreducible functions, but not necessarily of distinct degrees d_i, the preceding result is to be replaced by

$$D_m = p^{ne} \prod_i [d_i], \qquad e = \sum_i d_i(e_i - 1). \tag{34}$$

From $D_m > 1$ we infer that the fundamental equation has a root r such that $r^{p^{ni}}$ $(i = 0, 1, \cdots, m-1)$ are linearly independent with respect to the $GF[p^n]$. Hence, by (18), every root is of the form

$$\xi = \sum_{i=0}^{m-1} c_i r^{p^{ni}} \qquad (c\text{'s in } GF[p^n]).$$

Let D be the degree of the equation, irreducible in the $GF[p^n]$, which has the root r and hence also the roots $r^{p^{ni}}$. For $i = D$, the latter equals r. By the linear independence, $D \geqq m$.

Theorem. *Every irreducible factor in the $GF[p^n]$ of the fundamental equation is of degree a divisor of D, where D is not less than m and is the common degree of all the irreducible factors which do not divide a similar equation of lower degree. The fundamental equation is completely solvable in the $GF[p^{nD}]$, but not in a smaller field.*

16. We proceed to determine D. By the powers $p^n, p^{2n}, \cdots$ of (17),

$$\xi^{p^{nt}} = \sum_{i=0}^{m-1} a_i \xi^{p^{ni}} \equiv l_t(\xi) \qquad (t \geqq m).$$

We seek the least value D of t for which $l_t \equiv \xi$. Now, the coefficients of $\xi^{p^{n(m-1)}}, \cdots, \xi^{p^n}, \xi$ in l_t are the elements of the first row of S^{t-m+1}, where

$$S = \begin{Vmatrix} q_{m-1} & -q_{m-2} & q_{m-3} & \cdots & (-1)^{m-2} q_1 & (-1)^{m-1}\lambda \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{Vmatrix}.$$

If $l_t = \xi$, then $l_{t+1} = \xi^{p^n}, \cdots, l_{t+m-1} = \xi^{p^{n(m-1)}}$, and hence $S^t = 1$. Thus D is the period of the transformation of S. The minor of the element $\pm\lambda$ in the matrix S equals unity. Hence the characteristic determinant $(-1)^m \Delta(x)$ of S is its single invariant-factor. Hence,* if

$$(-1)^m \Delta(x) = F_k^{\kappa} F_l^{\lambda} \cdots,$$

where $F_k, F_l, \cdots$ are distinct irreducible functions in the $GF[p^n]$, the first having the roots $K_1, \cdots, K_k$, the second the roots $L_1, \cdots, L_l$, the transformation S has the canonical form

$$\eta'_{i1} = K_i \eta_{i1}, \ \eta'_{i2} = K_i(\eta_{i1} + \eta_{i2}), \ \eta'_{i3} = K_i(\eta_{i2} + \eta_{i3}), \cdots, \eta'_{i\kappa} = K_i(\eta_{i\kappa-1} + \eta_{i\kappa}),$$
$$\zeta'_{i1} = L_i \zeta_{i1}, \ \zeta'_{i2} = L_i(\zeta_{i1} + \zeta_{i2}), \ \zeta'_{i3} = L_i(\zeta_{i2} + \zeta_{i3}), \cdots, \zeta'_{i\lambda} = L_i(\zeta_{i\lambda-1} + \zeta_{i\lambda}), \cdots$$

*These Transactions, vol. 3 (1902), p. 291.

where $i = 1, \cdots, k$ in the first line, $i = 1, \cdots, l$ in the second, $\cdots$. The transformation S therefore has the maximum number of variables in each chain. Let κ be greatest of the exponents $\kappa, \lambda, \cdots$. Then the longest chain contains κ variables. Determine h so that $p^{h-1} < \kappa \leqq p^h$. Let d be the least common multiple of the exponents to which belong the roots $K_1, L_1, \cdots$. Then * $D = dp^h$.

Theorem. *The smallest field in which the fundamental equation is completely solvable is the* $GF[p^{nD}]$, $D = dp^h$, *where* d *is the least common multiple of the exponents to which belong the roots of the characteristic equation* $\Delta(x) = 0$, *while* p^h *is the least power of* p *which is equal to or greater than the maximum multiplicity of a root of* $\Delta(x) = 0$.

In the case of the classical equation $\xi^{p^m} - \xi = 0$, we have $\Delta(x) = x^m - 1$, so that $D = m$.

In case $\Delta(x)$ is a primitive irreducible function, we have $D = p^m - 1$. Thus the fundamental equation is the product of ξ and an irreducible equation.

The Interpretation of certain Invariants, § 17–22.

17. Since the determinant $[2m-2, 2m-4, \cdots, 4, 2, 0]$ is the product of the distinct † linear functions of m variables in the $GF[p^{2n}]$, its quotient by L_m is the product J_m of all distinct quadratic forms in the $GF[p^{2n}]$ on m variables which can be transformed into irreducible binary forms. Indeed, each linear factor of J_m is of the form $l_1 + \rho l_2$, where l_1 and l_2 are linear forms in the $GF[p^n]$, $l_2 \neq 0$, and ρ is a root of a quadratic equation irreducible in that field. If ρ' is the second root, $l_1 + \rho' l_2$ is a factor of J_m. The product of the two factors is a quadratic form in the $GF[p^n]$ which $x_1' = l_1$, $x_2' = l_2$ transforms into an irreducible binary form.

For $m = 2$, J_2 is the invariant Q_{21} of the fundamental system.

For $m = 3$, we have the following expression for J_3:

$$J_3 = Q_{31} Q_{32}^{p^n} - L_3^{p^n(p^n-1)}. \tag{35}$$

For proof, we expand the identically vanishing determinant

$$\begin{vmatrix} a_4 & b_4 & c_4 & 0 & 0 & 0 \\ a_3 & b_3 & c_3 & a_3 & b_3 & c_3 \\ a_2 & b_2 & c_2 & a_2 & b_2 & c_2 \\ a_1 & b_1 & c_1 & a_1 & b_1 & c_1 \\ a_0 & b_0 & c_0 & a_0 & b_0 & c_0 \\ 0 & 0 & 0 & a_2 & b_2 & c_2 \end{vmatrix}$$

* JORDAN, *Traité des Substitutions*, p. 127. Jordan's q is the present $h - 1$.

† Here and below we shall say that two functions are distinct if their ratio is not a constant.

by Laplace's method according to the minors of the first three columns and get

$$(36) \qquad (a_4b_3c_2)(a_2b_1c_0) - (a_4b_2c_1)(a_3b_2c_0) + (a_4b_2c_0)(a_3b_2c_1) \equiv 0.$$

Taking $a_i = x^{p^{ni}}$, $b_i = y^{p^{ni}}$, $c_i = z^{p^{ni}}$, and dividing by $L_3^{p^{n+1}}$, we get (35). Since (35) is an irreducible function of its arguments, we conclude that any irreducible binary quadratic form is equivalent to a constant multiple of any other irreducible binary quadratic form within G_3 and hence within G_2.

Invariants relating to Cubic Forms.

18. The product of the distinct linear functions of m variables in the $GF[p^{3n}]$, no one of which is a constant times a linear function in the $GF[p^n]$, equals

$$P_m = [3m-3, 3m-6, \cdots, 6, 3, 0]/L_m.$$

Each linear factor of P_m is of the form

$$\gamma = \sum_{i=1}^{m} \gamma_i x_i, \qquad \gamma_i \equiv c_{i0} + c_{i1}\rho + c_{i2}\rho^2,$$

where ρ is a root of a fixed irreducible cubic R in the $GF[p^n]$, and where the ratios of the γ_i do not all belong to the latter field.

If $m = 2$, the factors are $x_1 - \sigma x_2$, where σ is in the $GF[p^{3n}]$, but not in the $GF[p^n]$. Hence P_2 is the product of the distinct irreducible binary cubic forms in the $GF[p^n]$. See (42) below.

If $m \geqq 3$, the rank of the matrix (c_{ij}) is 3 or 2. In the first case $\sum c_{i0}x_i$, $\sum c_{i1}x_i$, $\sum c_{i2}x_i$ are linearly independent, and there exists a transformation of G_m which replaces γ by $x_1 + \rho x_2 + \rho^2 x_3$. The functions obtained from the latter by replacing ρ by either of the remaining roots of the cubic R are factors of P_m. Hence P_m contains as a factor the product K_m of all distinct m-ary cubic forms equivalent to a non-vanishing ternary cubic form.* If the rank is 2, the linear factor is equivalent to $x_1 - \rho x_2$. Hence $P_m = K_m C_m$, where C_m is the product of all distinct m-ary cubic forms equivalent to an irreducible binary form. Now, there are

$$(37) \qquad N = (p^{nm}-1)(p^{nm}-p^n)(p^{nm}-p^{2n})$$

sets of elements c_{ij} in the $GF[p^n]$ such that matrix (c_{ij}) is of rank 3. But two linear functions whose ratio is one of the $p^{3n}-1$ elements $\neq 0$ of the $GF[p^{3n}]$ give the same factor. Hence the degree of K_m is

$$(38) \qquad k_m = N/(p^{3n}-1).$$

The degree c_m of C_m is therefore $p_m - k_m$, where

$$(39) \qquad p_m = p^{3n(m-1)} - p^{n(m-1)} + p^{3n(m-2)} - p^{n(m-2)} + \cdots + p^{3n} - p^n.$$

*Dickson, Bulletin of the American Mathematical Society, vol. 14 (1908), p. 161.

19. We proceed to the evaluation of the invariant C_3 of degree

$$c_3 = (p^{3n} - p^n)(p^{2n} + p^n + 1) = p^n(p^{3n} - 1)(p^n + 1).$$

To this end we construct an integral function of the fundamental invariants (2) of G_3 which vanishes identically in y, z for $x = \rho y$, where

$$\rho^{p^{2n}} = \rho, \qquad \rho^{p^n} \neq \rho. \tag{40}$$

For $x = \rho y$, (1) gives

$$L_2 = (\rho^{p^n} - \rho) y^{p^n+1}, \qquad Q_{21} - k y^{p^{2n}-p^n}, \qquad k \equiv (\rho^{p^{2n}} - \rho)/(\rho^{p^n} - \rho).$$

In view of (40), we have

$$k^{p^n} = (\rho - \rho^{p^n})/(\rho^{p^{2n}} - \rho^{p^n}), \qquad k^{p^n+1} = (\rho - \rho^{p^{2n}})/(\rho^{p^{2n}} - \rho^{p^n}),$$

$$(\rho^{p^n} - \rho)^{p^{2n}-p^n} = (\rho^{p^{3n}} - \rho^{p^{2n}})/(\rho^{p^{2n}} - \rho^{p^n}) = k^{p^n+1},$$

$$Q_{21}^{p^n+1} = L_2^{p^{2n}-p^n}. \tag{41}$$

Since $p_2 = p^{3n} - p^n$ by (39), we conclude that *

$$P_2 = Q_{21}^{p^n+1} - L_2^{p^{2n}-p^n}. \tag{42}$$

The desired invariantive relation $C_3 = 0$ is obtained by the elimination of Q_{21} and L_2 from (41), (2_2) and (2_3). We have

$$Q_{31} = Q_{21} Q_{32}, \qquad L_2^{p^{2n}-p^n} = Q_{21}^{p^n+1} = (Q_{31}/Q_{32})^{p^n+1},$$

$$L_3^{p^{2n}-p^n} \left(\frac{Q_{32}}{Q_{31}}\right)^{p^n+1} = \left(\frac{L_3}{L_2}\right)^{p^{2n}-p^n} = (Q_{32} - Q_{21}^{p^n})^{p^n} = Q_{32}^{p^n} - \left(\frac{Q_{31}}{Q_{32}}\right)^{p^{2n}},$$

$$C_3 = L_3^{p^{2n}-p^n} Q_{32}^e - (Q_{31} Q_{32}^{p^n})^{p^n+1} + Q_{31}^e \qquad (e = p^{2n} + p^n + 1). \tag{43}$$

We proceed to express the invariant P_3 in terms of the fundamental invariants. With the notation of § 1, we obtain from (36),

$$[623][310] - [631][230] + [630][231] = 0,$$

$$[532][210] - [521][320] + [520][321] = 0,$$

$$[431][120] - [412][310] + [410][312] = 0.$$

We raise the second to the power p^n, the third to the power p^{2n}, and get

$$-[410]^{p^{2n}}[310] + [520]^{p^n}[320] - [630][210]^{p^n} = 0,$$

$$[310]^{p^{2n}}[210]^{p^n} - [410]^{p^{2n}}[320]^{p^n} + [520]^{p^n}[210]^{p^{2n}} = 0,$$

$$-[320]^{p^{2n}}[210]^{p^{2n}} + [310]^{p^{3n}}[310]^{p^{2n}} - [410]^{p^{2n}}[210]^{p^{3n}} = 0.$$

We eliminate $[520]^{p^n}$ and $[410]^{p^{2n}}$ linearly, divide by a power of $[210]$, and get

$$P_3 = [Q_{32}^{p^{2n}+p^{2n}} - Q_{31}^{p^{3n}}][Q_{31}^{p^n+1} - Q_{32} L_3^{p^{2n}-p^n}] - Q_{31} Q_{32}^{p^{3n}} L_3^{p^{3n}-p^{2n}}. \tag{44}$$

*Since Q_{21} is an absolute invariant of G_2 and L_3^r, $r = p^n - 1$, is the least power of L_2 giving an absolute invariant, any invariant factor of (42) must be of degree a multiple of $r(p^n + 1)$ and $p^{2n} - p^n$ and hence a multiple of $rp^n(p^n + 1)$. Thus P_2 is an irreducible invariant. Hence any irreducible binary cubic is equivalent within G_2 to a multiple of any other.

We readily verify the identity

$$Q_{32}^{p^{2n}+p^n} P_3 + Q_{31} C_3^{p^n} - Q_{31}^{p^{2n}} C_3 + Q_{32}^{p^{3n}+p^{2n}} C_3 \equiv 0. \tag{45}$$

Hence the product of all non-vanishing ternary cubics is

$$K_3 = -Q_{32}^{p^{2n}-p^n} + (Q_{31}^{p^{2n}} - Q_{31} C_3^{p^n-1})/Q_{32}^{p^{2n}+p^n}. \tag{46}$$

The last expression equals an integral function. By (43)

$$K_3 = -Q_{32}^{p^{2n}-p^n} - \sum_{i=1}^{p^n-1} (Q_{31}^{p^n+1} - Q_{32} L_3^{p^{2n}-p^n})^i Q_{32}^{p^{2n}+p^n)(i-1)} Q_{31}^{p^{2n}-ei}. \tag{46'}$$

Invariants relating to Quadratic Forms.

20. We next determine the invariantive expression for the product Q of all distinct ternary quadratic forms of non-vanishing discriminant* in the $GF[p^n]$. An integral function has the factor $y^2 - xz$ if and only if it vanishes identically in x and t when we set

$$y = tx, \qquad z = t^2 x.$$

For these values,

$$L_2 = x^{p^n+1}(t - t^{p^n}), \qquad Q_{21} = x^{rp^n}(t - t^{p^{2n}})/(t - t^{p^n}), \qquad r \equiv p^n - 1,$$
$$L_3 = x^e (t - t^{p^n})(t - t^{p^{2n}})(t^{p^n} - t^{p^{2n}}), \qquad e \equiv p^{2n} + p^n + 1.$$

By eliminating t, we get the two relations†

$$x^e L_3 = Q_{21} L_2^{p^n+2}, \qquad x^{p^{2n}} - x^{p^n} Q_{21} + x L_2^r = 0. \tag{47}$$

By means of the rth power of the former, we may express $x^{p^{2n}}$ as a multiple of x. Hence (47_2), its p^n-th power, and its p^{2n}-th power yield three linear relations between $x^{p^{2n}}$, x^{p^n}, x, the determinant of whose coefficients is a power of L_2 times

$$A Q_{21}^{p^{2n}-1} L_2^{rp^n} + B L_2^{r(p^{2n}-1)} + Q_{21}^{p^{2n}} L_3^r L_2^{p^{3n}-2p^n+1} - Q_{21}^{p^{2n}+2p^n} L_3^{rp^n} = 0,$$
$$A = L_3^{rp^n} Q_{21}^{p^n} + L_2^{p^{2n}-p^n}, \qquad B = L_3^{p^{2n}-1} + Q_{21}^{p^n} L_3^{rp^n} L_2^r. \tag{48}$$

We eliminate Q_{21} from A by means of (2_3), from B by means of (2_2):

$$A = Q_{31}^{p^n} L_2^{rp^n}, \qquad B = Q_{32} L_3^{rp^n} L_2^r.$$

Similarly, the last two terms of (48) equal

$$Q_{21}^{p^{2n}} \{(L_3^r/L_2^r - Q_{32})(Q_{31}^{p^n} L_2^{rp^n} - L_2^{p^{3n}-p^n}) + L_3^r L_2^{p^{3n}-2p^n+1}\}$$
$$= Q_{21}^{p^{2n}} \{L_3^r Q_{31}^{p^n} L_2^{r^2} + L_2^{rp^n} C\}, \qquad C \equiv Q_{32} L_2^{rp^{2n}} - Q_{32} Q_{31}^{p^n}.$$

In view of (2_3) the first term of the latter equals

$$Q_{21}^{p^{2n}-1}(Q_{31}^{p^n+1} L_2^{rp^n} - Q_{31}^{p^n} L_2^{2rp^n}).$$

The last term cancels the first term of (48). By (2_3),

$$C = -Q_{32} Q_{21}^{p^n} L_3^{rp^n}/L_2^{rp^n}.$$

*Semi-discriminant S_3 if $p = 2$, these Transactions, vol. 10 (1909), p. 134.

†The product of the second by L_2 is an identity in x, y, in view of (3).

Hence the new form of (48) is

$$L_2^{rp^{2n}} Q_{32} L_3^{rp^n} + Q_{21}^{p^{2n}-1} Q_{31}^{p^n+1} L_2^{rp^n} - Q_{32} Q_{21}^{p^{2n}+p^n} L_3^{rp^n} = 0.$$

The first and third terms equal $Q_{32} L_3^{rp^n} E^{p^n}$, where

$$E \equiv L_2^{rp^n} - Q_{21}^{p^n+1} = Q_{31} + Q_{32} L_2^{p^{2n}-1}/L_3^r - Q_{31} Q_{32} L_2^r/L_3^r,$$

in view of the product of $Q_{21}^{p^n}$ from (2_2) by Q_{21} from (2_3). Hence

$$(49)\quad Q_{21}^{p^{2n}-1} Q_{31}^{p^n+1} L_2^{rp^n} + L_3^{rp^n} Q_{31}^{p^n} Q_{32} + Q_{32}^{p^n+1} L_2^{p^{2n}-p^n} - Q_{31}^{p^n} Q_{32}^{p^n+1} L_2^{rp^n} = 0.$$

By eliminating Q_{21} between (2_2) and (2_3), we get

$$(50)\qquad L_2^{p^{2n}} - L_2^{p^{2n}} Q_{31}^{p^n} + L_2^{r} L_3^{rp^n} Q_{32} - L_2 L_3^{p^{2n}-1} = 0.$$

Multiply (49) by $L_2^{p^n}$ and eliminate $L_2^{p^{2n}}$ by (50). Then multiply by Q_{21}/L_2^r, replace Q_{21} by its value from (2_3), and $Q_{21}^{p^{2n}}$ by the p^n-th power of the value of $Q_{21}^{p^n}$ from (2_2). We get

$$(51)\quad \begin{aligned}(Q_{31} - L_2^{rp^n})(Q_{31}^{p^n} Q_{32} L_2^{p^n} L_3^{rp^n} - L_2^{p^n} L_3^{rp^n} Q_{32}^{p^n+2} + L_2 L_3^{p^{2n}-1} Q_{32}^{p^n+1}) \\ + L_3^r L_2^{p^{2n}-p^n+1} Q_{31}^{p^n+1} Q_{32}^{p^n} - L_2 L_3^{p^{2n}-1} Q_{31}^{p^n+1} = 0.\end{aligned}$$

Multiply (50) by $Q_{31} Q_{32}^{p^n+1} - Q_{31}^{p^n+1}$, add the result to (51); then divide by $L_2^{rp^n}$. We get

$$(52)\quad \begin{aligned}L_2^{p^{2n}-p^{2n}+p^n}(Q_{31} Q_{32}^{p^n+1} - Q_{31}^{p^n+1}) + L_2^{p^n}[L_3^{rp^n} Q_{32}^{p^n+2} - L_3^{rp^n} Q_{31}^{p^n} Q_{32} \\ - (Q_{31} Q_{32})^{p^n+1} + Q_{31}^{2p^n+1}] + L_2(L_3^r Q_{31}^{p^n+1} Q_{32}^{p^n} - L_3^{p^{2n}-1} Q_{32}^{p^n+1}) = 0.\end{aligned}$$

From the p^n-th power of (51) we eliminate $L_2^{p^{2n}}$ by (50) and obtain an equation involving the same three powers of L_2 as in (52). Eliminating the highest power of L_2 and dividing the resulting relation by $L_3^{rp^n}$, we obtain $FG = 0$, where

$$(53)\qquad F = L_2^{p^n}(Q_{31}^{p^n} - Q_{32}^{p^n+1}) + L_2 L_3^{p^n-1} Q_{32}^{p^n},$$

$$(54)\quad \begin{aligned}G = L_3^{p^{2n}\cdot p^n} Q_{32}^r + L_3^{p^{2n}-p^{2n}}(Q_{31}^{p^{2n}+1} Q_{32}^{p^n+1} - Q_{31} Q_{32}^{r+p^n} - Q_{31}^r) \\ - L_3^{p^{2n}-p^n} Q_{31}^{p^{2n}+p^n} Q_{32}^{p^{2n}+1} + Q_{31}^{r+p^n} Q_{32}^{p^{2n}}\end{aligned}$$

The factor F is extraneous, since it does not vanish for $x \neq 0$, t in the $GF[p^{2n}]$ but not in the $GF[p^n]$. Indeed, we then have

$$L_2 \neq 0,\ Q_{21} = 0,\ L_3 = 0,\ Q_{32} = 0,\ Q_{31} = L_2^{p^{2n}-p^n},\ F = L_2^{p^{2n}-p^{2n}+p^n}.$$

Hence the desired invariant Q is a factor of G. Now

$$(55)\quad G = J_3(Q_{31}^{p^{2n}+p^n} Q_{32}^{p^{2n}+1} - L_3^{p^{2n}-p^{2n}} Q_{32}^r) + J_3^{p^n}(Q_{31}^r - Q_{31}^{p^{2n}+1} Q_{32}^{p^n+1}),$$

where J_3 is defined by (35). *The invariant Q equals G/J_3.* This follows from the facts that any ternary quadratic form T of non-vanishing discriminant (semi-discriminant, if $p = 2$) is equivalent (*Linear Groups*, p. 158, p. 197)

under the total group G_3 to $c(y^2 - xz)$, and that the number of the forms T, no two with a constant ratio, is $N = p^{2n}(p^{3n} - 1)$, while the degree of Q is $2N$.

We may, however, give a direct proof that $Q = G/J_3$ and deduce the preceding facts as corollaries. This proof depends upon the fact that G/J_3 is not the product of two integral invariants of G_3. Since G/J_3 contains a term free of L_3, a factor f must contain such a term and hence be an absolute invariant of G_3. Hence the exponent of L_3 in each term of f is a multiple of $p^n - 1$. But the degrees of Q_{31} and Q_{32} are multiples of p^n. Hence the exponents of L_3 are multiples of $p^n(p^n - 1)$. Thus f is an integral function of J_3. By (35) and (55), we get

$$(55') \quad G/J_3 = Q_{31}^{p^n} Q_{32}^{p^{2n}+1} D^{p^n} + Q_{32}^{e} J_3^{p^n} + J_3^{p^n-1} Q_{31}^{p^{2n}+1} D, \qquad D \equiv Q_{31}^{p^n} - Q_{32}^{p^n+1}.$$

If this were reducible in J_3, then

$$(56) \qquad \sigma^{p^n} + \sigma Q_{31}^{p^{2n}} / Q_{32}^{p^{2n}+1} + Q_{32}^{p^n}$$

would be reducible in $\sigma = Q_{31} D/J_3$. But values of x, y, z may be found for which Q_{31} and Q_{32} take any assigned values (§ 8). Since the extraction of the p^n-th root is here uniquely possible, the coefficients of (56) may be given any assigned values. By § 13, values may be assigned such that (56) is the product of a linear and an irreducible factor of degree $p^n - 1$. Hence (55′) is either irreducible in its arguments or has a factor f_1 linear in J_3. Suppose the latter to be the case. The coefficient of J_3 is either 1 or Q_{32}^{e} in view of the part Q_{31}^{e} of the final term of (55′). If this coefficient is 1, the remaining terms of f_1 are of the same degree as J_3, so that

$$f_1 = J_3 - c Q_{31} Q_{32}^{p^n}.$$

But this is obviously not a factor of (55′). Next, for the factors

$$f_1 = Q_{32}^{e} J_3 + \lambda, \qquad J_3^{p^n-1} - c Q_{31} Q_{32}^{p^n} J_3^{p^n-2} + \cdots,$$

a comparison of the coefficient of $J_3^{p^n-1}$ of the product with that in (55′) gives

$$\lambda = c Q_{31} Q_{32}^{e+p^n} + Q_{31}^{p^{2n}+1} D.$$

Since λ contains the term Q_{31}^{e}, while e exceeds the exponent of Q_{31} in each part of the first term of (55′), f_1 is not a factor. Hence G/J_3 is not the product of two integral invariants of G_3 and thus equals Q.

It may happen that Q is the product of integral invariants of the subgroup G_3' of transformations of determinant unity, namely, that Q is a reducible in the arguments L_3, Q_{31}, Q_{32}. Since Q has a term involving only Q_{31} and Q_{32}, whose degrees are $\rho(p^n + 1)$ and ρp^n, where $\rho = p^n(p^n - 1)$, any factor f of Q is of degree a multiple of ρ. Thus the exponent a of L_3 in any term of f is such that ae is a multiple of ρ. The greatest common divisor of $e = p^{2n} + p^n + 1$ and ρ is 3 or 1 according as p^n is of the form $3l + 1$ or not. If $p^n \neq 3l + 1$,

the exponent a of L_3 is a multiple of ρ, and f is a function of J_3; but Q was shown to be irreducible in J_3. Hence *if* $p^n \neq 3l+1$, *any ternary quadratic form of non-vanishing discriminant is equivalent under* G_3' *to* $c(y^2-xz)$.

For $p^n = 3l+1$, Q is the product of three integral functions of $L_3^{\rho/3}$. This is in agreement with the fact that the types are now

$$c(y^2-kxz) \qquad (k=1,\ \epsilon,\ \epsilon^2),$$

where ϵ is a fixed not-cube (for example, a primitive root), while no one of the three types is equivalent under G_3' to a constant multiple of another type.

21. **Theorem.** *If* α *is a primitive root of the* $GF[p^n]$, $p^n > 2$, *and* β *is any element, the function*

$$\Sigma = \sigma^{p^n} - \alpha\sigma + \beta$$

is the product of a linear and an irreducible function of degree $p^n - 1$.

Let ξ and η be two distinct roots of $\Sigma = 0$. Let $z = \xi - \eta$. Then

$$z^{p^n} = \alpha z, \qquad z^{p^{2n}} = \alpha z^{p^n} = \alpha^2 z, \ \cdots, \qquad z^{p^{kn}} = \alpha^k z.$$

Since α belongs to the exponent $p^n - 1$, z belongs to the $GF[p^{kn}]$ if $k = p^n - 1$, but not if k is smaller.

Suppose that Σ has a factor f of degree $d\,(d < p^n)$, irreducible in the $GF[p^n]$. The roots of $f=0$ are ξ, ξ^{p^n}, $\xi^{p^{2n}}$, $\cdots$ and belong to the $GF[p^{dn}]$. The difference z of two of these roots is not zero and belongs to the latter field. Hence by the earlier result, $d = p^n - 1$.

For $p^n > 2$, we have $\alpha \neq 1$. But Σ vanishes if $\sigma = \beta/(\alpha - 1)$, an element of the $GF[p^n]$. Hence there is a linear factor.

For $p^n = 2$, the theorem holds for $\beta = 0$, but fails if $\beta = 1$.

22. We have determined the product Q of the distinct ternary quadratic forms not equivalent to a binary form, and the product J_3 of those equivalent to an irreducible binary form. A quadratic form equivalent to a reducible binary form is the product of two distinct linear forms; hence the product of all such ternary forms is $L_3^{p^{2n}+p^n}$. Finally, the product of the distinct quadratic forms equivalent to a unary form is L_3^2. Since $QJ_3 = G$, we conclude that the product of all distinct ternary quadratic forms is $GL_3^{p^{2n}+p^n+2}$. The degree of the latter product is $2(p^{6n}-1)/(p^n-1)$, as should be the case. The invariant G, given by (54), may be expressed as the following determinant:

$$(57) \qquad G = \begin{vmatrix} L_3^{p^{2n}-p^{2n}} & Q_{31} & 1 \\ L_3^{p^{2n}-p^{2n}} Q_{32}^{p^n+1} & L_3^{p^{2n}-p^n} Q_{32} & Q_{31}^{p^n} \\ Q_{31}^{p^{2n}+p^n} Q_{32}^{p^{2n}} & Q_{31}^{p^{2n}+1} & Q_{32}^{p^{2n}+p^n} \end{vmatrix}.$$

THE UNIVERSITY OF CHICAGO,
July, 1910.

LINEAR DIFFERENCE EQUATIONS AND THEIR ANALYTIC SOLUTIONS*

BY

R. D. CARMICHAEL

Introduction.

The first existence theorem for difference equations in which analytic solutions were treated was obtained by GUICHARD† who, in a paper published in 1887, proved that if $\phi(x)$ is any entire function whatever there exists another entire function $f(x)$ satisfying the relation

$$f(x+1)-f(x)=\phi(x).$$

Demonstrations of this theorem have also been given by APPELL‡ and HURWITZ.§ HURWITZ further showed how to solve the equation

$$\phi(x)f(x+1)-\chi(x)f(x)=\psi(x),$$

where $\phi(x)$, $\chi(x)$, $\psi(x)$ are meromorphic functions.

MELLIN‖ has considered the nature of the solution of

$$f(x+1)-r(x)f(x)=s(x),$$

where $r(x)$ and $s(x)$ are rational functions.

BARNES¶ has contributed an interesting study of the equation

$$\phi(x)f(x+\omega)-\chi(x)f(x)=\psi(x),$$

where ω is any constant different from zero and $\phi(x)$, $\chi(x)$, $\psi(x)$ are entire functions.

WATSON** has considered the equation of the second order

$$A(x)f(x+1)-B(x)f(x)+C(x)f(x-1)=0,$$

* Presented to the Society September 6, 1910.

† Annales de l'École Normale supérieure, ser. 3, vol. 4 (1887), p. 361.

‡ Journal de Mathématiques, ser. 4, vol. 7 (1891), p. 157, especially chapter I, pp. 159–176.

§ Acta Mathematica, vol. 20 (1897), p. 285.

‖ Acta Mathematica, vol. 15 (1891), p. 317.

¶ Proceedings of the London Mathematical Society, ser. 2, vol. 2 (1905), p. 438.

** Proceedings of the London Mathematical Society, ser. 2, vol. 8 (1910), p. 125.

with some restrictions on $A(x)$, $B(x)$, $C(x)$, the object of his investigation being to obtain a solution which is of use in applications to the theory of linear differential equations. Two analytic solutions are obtained, but the question of their independence is left unanswered.

Finally, GALBRUN* has employed the Laplace transformation which carries a linear difference equation with polynomial coefficients into a differential equation, and by means of this transformation has obtained important existence theorems for the case in which the difference equation has polynomial coefficients.

The primary object of the present paper is to prove that there exists a fundamental system of simple analytic solutions of the system of n linear homogeneous difference equations

$$(A) \qquad G_i(x+1) = x^{\alpha} \sum_{j=1}^{n} a_{ij}(x) G_j(x) \qquad (i=1, \cdots, n),$$

the known quantities entering into the equations being defined as follows:

1) α is a constant;

2) the functions $a_{ij}(x)$ are single-valued and

$$a_{ij}(x) = a_{ij} + a'_{ij}x^{-1} + a''_{ij}x^{-2} \cdots \qquad (i,j=1, \cdots, n) \qquad |x| > R';$$

3) the constants a_{ij} are such that the roots of the equation

$$|a_{ij} - \delta_{ij}\rho| = 0, \qquad \delta_{ij} = \begin{cases} 0 \text{ if } i \neq j, \\ 1 \text{ if } i = j, \end{cases}$$

are in absolute value different from each other and from zero.

In § 1 a form of the method of successive approximation is developed in connection with a single equation of the first order and by means of it a study is made of the nature of a simple particular solution of the equation.

The methods of § 1 are readily extended in § 2 in such a way that they lead to a similar solution of the normal system

$$(B) \qquad f_i(x+1) - a_i\left(1+\frac{1}{x}\right)^{m_i} f_i(x) = \sum_{j=1}^{n} \phi_{ij}(x) f_j(x) \qquad (i=1, \cdots, n),$$

where

$$0 < |a_1| < |a_2| < \cdots < |a_n|$$

and

$$\phi_{ij}(x) = \phi''_{ij}x^{-2} + \phi'''_{ij}x^{-3} + \cdots \qquad (i,j=1, \cdots, n) \qquad |x| \geqq R > 1.$$

A method of induction in § 3 leads to the determination of a fundamental system of solutions of (B) and to the development of important properties of the functions of which it is composed.

In § 4 it is shown that system (A) can be reduced to the normal form (B)

*Comptes rendus, vol. 148 (1909), p. 905; vol. 149 (1909), p. 1046; vol. 150 (1910), p. 206; vol. 151 (1910), p. 1114.

and thus the general existence theorem for (A) is obtained. Finally, an application of this result is made in deriving the general existence theorem for a single equation of the nth order.

I desire to express my cordial thanks to Professor G. D. Birkhoff for valuable suggestions and encouragement in the preparation of the paper.

§ 1. *The method of successive approximation for a single homogeneous equation of the first order.*

We shall begin by considering a single homogeneous equation of the first order in the normal form *

$$f(x+1) - a\left(1+\frac{1}{x}\right)^m f(x) = \phi(x) f(x), \qquad a \neq 0, \tag{1}$$

or

$$f(x+1) = \psi(x) f(x), \qquad \psi(x) \equiv a\left(1+\frac{1}{x}\right)^m + \phi(x),$$

where

$$\phi(x) = \phi'' x^{-2} + \phi''' x^{-3} + \cdots, \qquad \text{for } |x| \geqq R > 1. \tag{2}$$

We assume that $\psi(x)$ is single-valued and analytic at all points of the complex plane where it is defined, and that that determination of $(1+1/x)^m$ is taken which approaches 1 as x approaches infinity. The sequence of equations

$$\begin{aligned} &f^{(1)}(x+1) - a\left(1+\frac{1}{x}\right)^m f^{(1)}(x) = 0, \\ &f^{(2)}(x+1) - a\left(1+\frac{1}{x}\right)^m f^{(2)}(x) = \phi(x) f^{(1)}(x), \\ &f^{(3)}(x+1) - a\left(1+\frac{1}{x}\right)^m f^{(3)}(x) = \phi(x) f^{(2)}(x), \\ &\quad \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots, \end{aligned} \tag{3}$$

will serve to define a sequence of approximation functions $f^{(1)}(x), f^{(2)}(x), \cdots$. A particular solution of the first equation is evidently $a^x x^m$. All the other equations of the set have the general non-homogeneous form

$$g(x+1) - a\left(1+\frac{1}{x}\right)^m g(x) = \eta(x). \tag{4}$$

* It is easy to reduce the general first order equation

$$G(x+1) = x^\alpha(\theta + \theta' x^{-1} + \theta'' x^{-2} + \cdots) G(x), \qquad \theta \neq 0,$$

to this form. Put

$$G(x) = \{\Gamma(x)\}^\alpha f(x).$$

Then

$$f(x+1) = (\theta + \theta' x^{-1} + \theta'' x^{-2} + \cdots) f(x);$$

and for $|x|$ sufficiently large this evidently may be put in the form (1).

One readily obtains a formal solution of this equation as follows: Let

$$g(x) = a^x x^m \bar{g}(x),$$

where $a^x x^m$ has any determination fixed by making a cut along the negative axis of reals in the x-plane. Substituting in (4) this value of $g(x)$ and dividing by $a^{x+1}(x+1)^m$ one has

$$\bar{g}(x+1) - \bar{g}(x) = \frac{\eta(x)}{a^{x+1}(x+1)^m},$$

an equation which has the formal solution

$$\bar{g}(x) = -\frac{\eta(x)}{a^{x+1}(x+1)^m} - \frac{\eta(x+1)}{a^{x+2}(x+2)^m} - \frac{\eta(x+2)}{a^{x+3}(x+3)^m} - \cdots.$$

Hence

$$g(x) = -\frac{\eta(x)}{a\left(1+\frac{1}{x}\right)^m} - \frac{\eta(x+1)}{a^2\left(1+\frac{2}{x}\right)^m} - \frac{\eta(x+2)}{a^3\left(1+\frac{3}{x}\right)^m} - \cdots. \tag{5}$$

Now

$$a^r\left(1+\frac{r}{x}\right)^m = \lambda(x)\lambda(x+1)\cdots\lambda(x+r-1),$$

where

$$\lambda(x) = a\left(1+\frac{1}{x}\right)^m,$$

and therefore (5) may be written in the form *

$$g(x) = -\sum_{i=0}^{\infty} \frac{\eta(x+i)}{\lambda(x)\lambda(x+1)\cdots\lambda(x+i)}. \tag{6}$$

This yields not merely a formal but an actual solution for any values of x for which it converges; and if $\eta(x)$ is analytic, then (by Weierstrass's theorem) it yields an analytic solution throughout any two-dimensional continuum where it converges uniformly.

By the aid of (6) we obtain a sequence of formal solutions $f^{(i)}(x)$ satisfying (3) identically. Employing the notation

$$S_x(\chi) = -\sum_{i=0}^{\infty} \frac{\chi(x+i)}{\lambda(x)\lambda(x+1)\cdots\lambda(x+i)}$$

and using for each equation that particular formal solution which is obtained by adding the solution $a^x x^m$ of the homogeneous equation to the solution derived from (6), we have

$$f^{(1)}(x) = a^x x^m,$$
$$f^{(2)}(x) = a^x x^m + S_x(\phi a^x x^m),$$
$$f^{(3)}(x) = a^x x^m + S_x\{\phi a^x x^m + \phi S_x(\phi a^x x^m)\},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

*Cf. MELLIN, Acta Mathematica, vol. 15 (1891), p. 319.

It is easy to see that this leads to a formal solution $f_1(x)$ of (1), defined by the series

$$f_1(x) = a^x x^m + S_x(\phi a^x x^m) + S_x\{\phi S_x(\phi a^x x^m)\} + S_x[\phi S_x\{\phi S_x(\phi a^x x^m)\}] + \cdots. \tag{7}$$

That this series formally satisfies (1) we may verify by forming the difference $f_1(x+1) - a(1+1/x)^m f_1(x)$ and effecting a reduction of the resulting series by means of the general formula

$$S_{x+1}(\chi) - a\left(1+\frac{1}{x}\right)^m S_x(\chi) = \chi.$$

Consequently whenever all the series S_x in the terms of (7) and also the series (7) itself converge, this series represents a solution of (1).

In studying the nature of the formal solution (7) (and in the work of the succeeding sections also) it will be convenient to have names assigned to certain regions of the plane about which we shall have to speak often. Let R be the

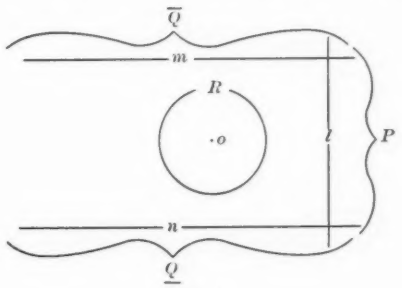

FIG. 1.

circle $|x| = R$. Let l be a line cutting the positive axis of reals at right angles and not cutting R. The part of the finite plane to the right of and including l will be called a P-region. Let m and n be parallel to the axis of reals, m lying above and n below R. The part of the finite plane lying above and including m will be named a $\bar{Q}$-region; that lying below and including n, a $\underline{Q}$-region; these two together, a Q-region. A region formed by the combination of the P- and Q-regions will be called a D-region. The part of the finite plane not included within D will be called the E-region corresponding to D. It is scarcely necessary to remark that $\bar{Q}$ and $\underline{Q}$ have each a part in common with P.

In what follows immediately we are to prove the existence of $f_1(x)$ and develop its properties in particular regions P_1, Q_1, D_1, E_1; for convenience all these regions are defined at once. For any positive constant c, less than $|a|$, there

exists an R' such that

$$\left| a\left(1+\frac{1}{x}\right)^m \right| > c, \qquad \text{for } |x| > R'.$$

From the nature of the function $\phi(x)$ it follows that there exists an M such that

$$|\phi(x)| < \frac{Mc}{|x|^2}, \qquad \text{for } |x| \geqq R.$$

If one writes

$$x = u \pm v\sqrt{-1}$$

where v is positive and both u and v are real, it is now clear that one may choose particular regions P, Q, D, E—call them P_1, Q_1, D_1, E_1 respectively—such that

$$|\phi(x)| < \frac{Mc}{|x|^2}, \qquad \left| a\left(1+\frac{1}{x}\right)^m \right| > c, \qquad \text{for } x \text{ in } D_1; \tag{8}$$

$$u > M+1, \qquad \text{for } x \text{ in } P_1; \tag{9}$$

$$\frac{A}{v} < \frac{M\pi}{v} + \frac{2M}{v^2} < 1, \qquad \text{for } x \text{ in } Q_1, \ A \text{ being a constant}; \tag{10}$$

$$a\left(1+\frac{1}{x}\right)^m + \phi(x) \neq 0, \qquad \text{for } x \text{ in } D_1. \tag{11}$$

Let us consider the function

$$\bar{S}_x(\phi a^x x^m) \equiv \sum_{i=0}^{\infty} \left| \frac{\phi(x+i)a^{x+i}(x+i)^m}{\lambda(x)\lambda(x+1)\cdots\lambda(x+i)} \right| = \sum_{i=0}^{\infty} \left| \frac{\phi(x+i)a^x x^m}{\lambda(x+i)} \right|. \tag{12}$$

Employing inequalities (8) one has the relation *

$$\sum_{i=0}^{\infty} \left| \frac{\phi(x+i)a^x x^m}{\lambda(x+i)} \right| \ll \sum_{i=0}^{\infty} \frac{M|a^x x^m|}{(u+i)^2+v^2} \tag{13}$$

subsisting throughout D_1. The series of the last member of (13) is evidently uniformly convergent when x lies in any closed region in D_1. The same then is true of the series in the first member, and hence also of the series in (12). Therefore $S_x(\phi a^x x^m)$ is a uniformly convergent series in the same closed region and hence, in accordance with a well-known theorem of Weierstrass, represents in this region an analytic function of x. From this it follows that the first and second terms of the series in (7) represent functions which are analytic in D_1.

In order to show that the remaining terms are analytic in the same region it is necessary to know a bound to the magnitude of $|S_x(\phi a^x x^m)|$ as x varies. In carrying out the needful reckoning it is convenient to treat the regions P_1 and Q_1 separately.

* The symbol $\ll$ is to be read *is less term by term than.*

First, let us consider the region P_1. Of the two series

$$\sum_{i=0}^{\infty} \frac{M}{(u+i)^2+v^2}, \qquad \sum_{i=0}^{\infty} \frac{M}{(u+i)^2}, \quad \text{for } x \text{ in } P_1,$$

the terms of the first in order are equal to or less than the corresponding terms of the second. But the latter series is less than the integral

$$\int_{u-1}^{\infty} \frac{M}{z^2}\, dz = \frac{M}{u-1};$$

and therefore

$$\bar{S}_x(\phi a^x x^m) < |a^x x^m| \frac{M}{u-1}. \tag{14}$$

Hence

$$|S_x(\phi a^x x^m)| < |a^x x^m| \frac{M}{u-1}.$$

Using this result and making an argument similar to that associated with inequality (13) one may show that $S_x\{\phi S_x(\phi a^x x^m)\}$ is analytic throughout P_1. Again, in view of (14) we have

$$\bar{S}_x\{\phi \bar{S}_x(\phi a^x x^m)\} < \bar{S}_x\left\{\phi |a^x x^m| \frac{M}{u-1}\right\} < \frac{M}{u-1}\, \bar{S}_x(\phi a^x x^m) < |a^x x^m| \frac{M^2}{(u-1)^2}.$$

Similarly it may be proved that $S_x[\phi S_x\{\phi S_x(\phi a^x x^m)\}]$ is analytic in P_1; an upper bound for the value of $\bar{S}_x[\phi \bar{S}_x\{\phi \bar{S}_x(\phi a^x x^m)\}]$ may be obtained; and so on. Hence in series (7) every term is analytic throughout P_1; moreover the following inequality has been established for x in P_1:

$$\bar{S}_x(\phi a^x x^m) + \bar{S}_x\{\phi \bar{S}_x(\phi a^x x^m)\} + \bar{S}_x[\phi \bar{S}_x\{\phi \bar{S}_x(\phi a^x x^m)\}] + \cdots \ll \frac{M|a^x x^m|}{u-1} + \frac{M^2|a^x x^m|}{(u-1)^2} + \frac{M^3|a^x x^m|}{(u-1)^3} + \cdots. \tag{15}$$

From (9) it follows that the second member of (15) is absolutely and uniformly convergent throughout any closed region in P_1; and therefore the same is true of the first member. Hence series (7) is uniformly and absolutely convergent throughout this region. But its terms are analytic functions of x; and therefore, by Weierstrass's theorem, its sum $f_1(x)$ is an analytic function of x throughout P_1. Evidently, then, $f(x) = f_1(x)$ is a solution of (1).

A comparison of (7) and (15) shows that the following inequalities are valid for x in P_1:

$$|a^x x^m|\left\{1 - \frac{M}{u-1} - \frac{M^2}{(u-1)^2} - \cdots\right\} < |f_1(x)| < |a^x x^m|\left\{1 + \frac{M}{u-1} + \frac{M^2}{(u-1)^2} + \cdots\right\}.$$

Hence we have

$$(16) \qquad |a^x x^m| \frac{u-2M-1}{u-M-1} < |f_1(x)| < |a^x x^m| \frac{u-1}{u-M-1},$$

a set of fundamental inequalities bounding the increase or decrease of $f_1(x)$ throughout P_1.

Again using relation (13) as a point of departure, we obtain similar results valid in Q_1. In this region v is different from zero. It is evident that

$$\sum_{i=0}^{\infty} \frac{M}{(u+i)^2+v^2} < \sum_{i=-\infty}^{\infty} \frac{M}{(u+i)^2+v^2} \leqq 2\left\{ M\int_0^{\infty} \frac{dz}{z^2+v^2} + \frac{M}{v^2} \right\} = \frac{M\pi}{v} + \frac{2M}{v^2} < \frac{A}{v},$$

A being a properly chosen constant. Comparing this result with (12) and (13) one has

$$(17) \qquad |S_x(\phi a^x x^m)| \leqq \bar{S}_x(\phi a^x x^m) < |a^x x^m| \frac{A}{v}.$$

On account of (10) and (18) it is clear that one may employ an argument similar to that associated with (13) to show that $S_x\{\phi S_x(\phi a^x x^m)\}$ is an analytic function of x in Q_1. Again, on account of (17) one has

$$(18) \quad \bar{S}_x\{\phi \bar{S}_x(\phi a^x x^m)\} < \bar{S}_x\left\{ \phi |a^x x^m| \frac{A}{v} \right\} = \frac{A}{v}\, \bar{S}_x(\phi a^x x^m) < |a^x x^m| \frac{A^2}{v^2}.$$

In like manner it may be shown that the function $S_x[\phi S_x\{\phi S_x(\phi a^x x^m)\}]$ is analytic throughout Q_1; also, an upper bound for the value of

$$\bar{S}_x[\phi \bar{S}_x\{\phi \bar{S}_x(\phi a^x x^m)\}]$$

may be obtained; and so on. Hence every term in series (7) is analytic in Q_1. Moreover, for this region the following relation exists:

$$(19) \quad \bar{S}_x(\phi a^x x^m) + \bar{S}_x\{\phi \bar{S}_x(\phi a^x x^m)\} + \bar{S}_x[\phi \bar{S}_x\{\phi \bar{S}_x(\phi a^x x^m)\}] + \cdots$$
$$\ll |a^x x^m| \frac{A}{v} + |a^x x^m| \frac{A^2}{v^2} + |a^x x^m| \frac{A^3}{v^3} + \cdots.$$

By a method similar to that employed in the previous case it is now easy to show that $f_1(x)$ is analytic in Q_1, and that throughout this region it is bounded as in the inequalities

$$(20) \qquad |a^x x^m| \frac{v-2A}{v-A} < |f_1(x)| < |a^x x^m| \frac{v}{v-A}.$$

It remains to determine the nature of $f_1(x)$ in the region E_1. For this study series (7) does not furnish a convenient means. We proceed as follows: If we solve (1) for $f(x)$ and in the result write $x-1$ for x we have

$$(21) \qquad f(x-1) = \bar{\psi}(x-1) f(x)$$

where

$$\bar{\psi}(x) = \{\psi(x)\}^{-1}. \tag{22}$$

By means of (21), the solution $f_1(x)$ which is known to exist in P_1 can be extended across the plane to the left; and in this way the nature of $f_1(x)$ in E_1 is determined.

Consider the set of points $[S]$ which is formed of the set $[\alpha]$ and of the sets $[\alpha - i]$, $i = 1, 2, 3, \cdots$, where $[\alpha]$ is the set of singularities of $\bar{\psi}(x)$. A point $\alpha - i$ is said to be *congruent to α on the left;* in a similar way *congruence on the right* is defined. It is easy to see that $f_1(x)$ is analytic at every point x' not belonging to $[S]$. For, by (21),

$$f_1(x') = \bar{\psi}(x')\bar{\psi}(x'+1)\cdots\bar{\psi}(x'+\nu-1)f_1(x'+\nu).$$

ν can be so chosen that $x'+\nu$ lies in P_1. For such a value of ν, $f_1(x)$ is analytic at $x'+\nu$; also, $\bar{\psi}(x)$ is analytic at each of the points x', $x'+1$, $\cdots$, $x'+\nu-1$. Therefore $f_1(x)$ is analytic at x'. Combining this with previous results, we see that $f_1(x)$ is analytic throughout the finite plane except at the singularities $[\alpha]$ of $\bar{\psi}(x)$ and the points congruent to them on the left; at these points its character depends upon the nature of the particular $\bar{\psi}(x)$ involved.

Let each point of $[S]$ be inclosed by a small circle of radius ϵ having the point as its center. Denote by $E_{1\epsilon}$ the whole of that part of E_1 no point of which is within one of these small circles.

Inequalities bounding the increase or decrease of $f_1(x)$ for x in $E_{1\epsilon}$ may be found as follows: Consider any positive constants a_- and a_+ satisfying the relations

$$a_- < |a| < a_+.$$

Since

$$\lim_{x=\infty} \left\{ a\left(1+\frac{1}{x}\right)^m + \phi(x) \right\} = a,$$

it is clear that r may be chosen so that

$$a_+ > \left| a\left(1+\frac{1}{x}\right)^m + \phi(x) \right| > a_-, \quad \text{for } |x| > r,$$

and also so that the circle $|x| = r$ cuts the boundary of E_1 twice on the left of the origin and at no other point. Since $f_1(x)$ is everywhere analytic in $E_{1\epsilon}$ it follows that there exist constants N_1 and N_2 such that

$$N_1 \leqq |f_1(x'')| < N_2, \qquad \text{for } x'' \text{ in } E_{1\epsilon} \text{ and } r \leqq |x''| \leqq r+1.$$

But (21) yields the equation

$$f_1(x''-\mu) = \bar{\psi}(x''-\mu)\bar{\psi}(x''-\mu+1)\cdots\psi(x''-1)f_1(x'').$$

Hence we have

$$N_1 a_+^{-\mu} \leqq |f(x''-\mu)| < N_2 a_-^{-\mu}, \qquad \text{for } x'' \text{ in } E_{1\epsilon} \text{ and } r \leqq |x''| \leqq r+1.$$

As μ varies over the range $\mu = 0, 1, 2, \cdots$, $x''-\mu$ runs over all points in $E_{1\epsilon}$ and outside of the circle $|x| = r$. Also, $f_1(x)$ is finite in the part of $E_{1\epsilon}$ which is in the circle $|x| = r$. Hence it is clear that there exist constants N_1 and N_2 such that

$$N_1 |a_+^x| \leqq |f_1(x)| < N_2 |a_-^x|, \quad \text{for } x \text{ in } E_{1\epsilon}, \tag{23}$$

the result sought.

So far we have said nothing of the position of the zeros of $f_1(x)$. By means of equation (1) we shall show that they can occur only at the singularities of $\psi(x)$ and at points congruent to them on the left. We have

$$f_1(x'+\mu) = \psi(x'+\mu-1)\psi(x'+\mu-2)\cdots\psi(x')f_1(x'),$$

where μ is a positive integer. From inequality (16) it follows that for every x' there exists a μ such that $f_1(x'+\mu)$ is different from zero. Hence $f_1(x')$ can be zero only when one at least of the factors $\psi(x'), \psi(x'+1), \cdots, \psi(x'+\mu-1)$ is infinite: and therefore the zeros of $f_1(x)$ must all be contained in the set of points composed of the singularities of $\psi(x)$ and the points congruent to them on the left.

The principal results contained in the section may be enunciated as follows:

The difference equation

$$f(x+1) = \psi(x)f(x) \text{ or } f(x-1) = \bar{\psi}(x-1)f(x), \qquad \bar{\psi}(x) \equiv \{\psi(x)\}^{-1},$$

in which $\psi(x)$ is single-valued and

$$\psi(x) = a\left(1+\frac{1}{x}\right)^m + \phi(x), \qquad \phi(x) = \phi'' x^{-2} + \phi''' x^{-3} + \cdots, \text{ for } |x| \geqq R > 1,$$

has a particular solution $f_1(x)$ which is analytic throughout the finite plane except at the singularities $[\alpha]$ of $\bar{\psi}(x)$ and the points congruent to them on the left, and which can vanish only at the singularities $[\beta]$ of $\psi(x)$ and at points congruent to them on the left. If D_1 is defined by relations (8) to (11), then throughout any closed region in D_1 this solution is representable as a uniformly converging series in the form

$$f_1(x) = a^x x^m + S_x(\phi a^x x^m) + S_x\{\phi S_x(\phi a^x x^m)\} + S_x[\phi S_x\{\phi S_x(\phi a^x x^m)\}] + \cdots.$$

The increase or decrease of $f_1(x)$ for x in the corresponding regions P_1 and Q_1 is bounded as in the inequalities

$$|a^x x^m| \frac{u-2M-1}{u-M-1} < |f_1(x)| < |a^x x^m| \frac{u-1}{u-M-1}, \quad \text{for } x \text{ in } P_1;$$

$$|a^x x^m| \frac{v-2A}{v-A} < |f_1(x)| < |a^x x^m| \frac{v}{v-A}, \quad \text{for } x \text{ in } Q_1.$$

Also, for any positive constants a_- and a_+ satisfying the relations

$$a_- < |a| < a_+$$

there exist other constants N_1, N_2 such that

$$N_1|a_+^x| \leqq |f_1(x)| < N_2|a_-^x|, \quad \text{for } x \text{ in } E_{1\epsilon}.$$

REMARK. About each statement in the conclusion of this theorem it should be observed that, insofar as the statement refers to the region D_1 or any part of it, it is independent of the nature of $\phi(x)$ in the region exterior to D_1. More explicitly: *If $\phi(x)$ is any function which is analytic in some D-region and if also*

$$|\phi(x)| < \frac{Mc}{|x|^2}, \quad \text{for } x \text{ in } D,$$

then there exist regions P_1, Q_1, D_1 having as before the properties (8) *to* (10), *and there is a particular solution $f_1(x)$ of the difference equation having in D_1 the same properties as the solution $f_1(x)$ of the equation in the theorem.* These conclusions follow from the preceding discussion without change of argument.

§ 2. *The method of successive approximation for a normal system of n equations. Properties of the solution thus obtained.*

Let us consider the system of n linear difference equations of the first order in the normal form

$$f_i(x+1) - a_i\left(1+\frac{1}{x}\right)^{m_i} f_i(x) = \sum_{j=1}^{n} \phi_{ij}(x) f_j(x) \qquad (i=1, \cdots, n), \tag{24}$$

or

$$f_i(x+1) = \sum_{j=1}^{n} \psi_{ij}(x) f_j(x), \qquad \psi_{ij}(x) \equiv \delta_{ij} a_i\left(1+\frac{1}{x}\right)^{m_i} + \phi_{ij}(x),$$

where

$$0 < |a_1| < |a_2| < \cdots < |a_n| \tag{25}$$

and

$$\phi_{ij}(x) = \phi_{ij}'' x^{-2} + \phi_{ij}''' x^{-3} + \cdots \qquad (i,j=1, \cdots, n), \quad \text{for} \quad |x| \geqq R > 1. \tag{26}$$

We assume that $\psi_{ij}(x)$ is single-valued. If we solve (24) for $f_i(x)$ in terms of $f_i(x+1)$, $i=1, \cdots, n$, and in the result write $x-1$ for x, we obtain

$$f_i(x-1) = \sum_{j=1}^{n} \bar{\psi}_{ij}(x-1) f_j(x) \qquad (i=1, \cdots, n), \tag{27}$$

$\bar{\psi}_{ij}(x)$ having the form

$$\bar{\psi}_{ij}(x) = \frac{\alpha_{ij}(x)}{\Delta} \tag{28}$$

where Δ is the determinant

$$\Delta \equiv \left| \delta_{ij} a_i\left(1+\frac{1}{x}\right)^{m_i} + \phi_{ij}(x) \right|$$

and $\alpha_{ij}(x)$ is the cofactor of the element in the jth column and the ith row of Δ.

The object of this section is to obtain a particular solution of (24) and to study its properties throughout the plane.

On account of (25) and (26) it is clear that there exist particular regions P_1, Q_1, D_1, E_1 and constants c, M and A such that the following inequalities are true:

$$(30)\quad |\phi_{ij}(x)| < \frac{Mc}{n|x|^2}, \qquad \left|a_i\left(1+\frac{1}{x}\right)^{m_i}\right| > c \quad (i,j=1,\cdots,n), \quad \text{for } x \text{ in } D_1;$$

$$(31)\quad \left|a_1\left(1+\frac{1}{x}\right)^{m_1}\right| < \left|a_i\left(1+\frac{1}{x}\right)^{m_i}\right| \quad (i=2,\cdots,n), \quad \text{for } x \text{ in } D_1;$$

$$(32)\quad u > M+1, \quad \text{for } x \text{ in } P_1, \quad \text{where } x = u \pm v\sqrt{-1};$$

$$(33)\quad \frac{A}{v} < \frac{M\pi}{v} + \frac{2M}{v^2} < 1, \quad \text{for } x \text{ in } Q_1;$$

$$(34)\quad \Delta \neq 0, \quad \text{for } |x| \geqq \bar{R} \geqq R.$$

In the study of our system of equations these regions are treated separately.

It will be convenient to employ the notation

$$S_{xi}(\chi) \equiv -\sum_{\nu=0}^{\infty} \frac{\chi(x+\nu)}{\lambda_i(x)\lambda_i(x+1)\cdots\lambda_i(x+\nu)}, \qquad \lambda_i(x) \equiv a_i\left(1+\frac{1}{x}\right)^{m_i};$$

also we write

$$u_i \equiv C_i a_i^x x^{m_i},$$

where C_i is any periodic function of x of period 1 and analytic throughout D_1.

The form of the method of successive approximation employed in the preceding section is readily generalized so as to lead to a particular solution of (24). Consider the set of systems each of n linear equations, all except the first being non-homogeneous:

$$\begin{aligned}
&f_i^{(1)}(x+1) - a_i\left(1+\frac{1}{x}\right)^{m_i} f_i^{(1)}(x) = 0,\\
&f_i^{(2)}(x+1) - a_i\left(1+\frac{1}{x}\right)^{m_i} f_i^{(2)}(x) = \sum_{j=1}^{n} \phi_{ij}(x) f_j^{(1)}(x), \qquad (i=1,\cdots,n).\\
&f_i^{(3)}(x+1) - a_i\left(1+\frac{1}{x}\right)^{m_i} f_i^{(3)}(x) = \sum_{j=1}^{n} \phi_{ij}(x) f_j^{(2)}(x),\\
&\quad\cdots\cdots\cdots\cdots\cdots\cdots\cdots,
\end{aligned}$$

Proceeding as in the foregoing section, one writes out in order formal solutions

of these systems, obtaining thus the following set of approximation functions:

$$f_i^{(1)}(x) = u_i.$$

$$f_i^{(2)}(x) = u_i + S_{xi}\left(\sum_{j=1}^{n} \phi_{ij} u_j\right),$$

$$f_i^{(3)}(x) = u_i + S_{xi}\left(\sum_{j=1}^{n} \phi_{ij} u_j\right) + S_{xi}\left\{\sum_{j=1}^{n} \phi_{ij} S_{xj}\left(\sum_{k=1}^{n} \phi_{jk} u_k\right)\right\}, \qquad (i = 1, \cdots, n).$$

. . . . . .

It is easy to verify by actual substitution that a solution of system (24) is obtained in the limit functions (if they exist) of the sequences $f_i^{(1)}, f_i^{(2)}, f_i^{(3)}, \cdots, i = 1, \cdots, n$; that is, in

$$\begin{aligned} f_i(x) = u_i &+ S_{xi}\left(\sum_{j=1}^{n} \phi_{ij} u_j\right) + S_{xi}\left\{\sum_{j=1}^{n} \phi_{ij} S_{xj}\left(\sum_{k=1}^{n} \phi_{jk} u_k\right)\right\} \\ &+ S_{xi}\left[\sum_{j=1}^{n} \phi_{ij} S_{xj}\left\{\sum_{k=1}^{n} \phi_{jk} S_{xk}\left(\sum_{l=1}^{n} \phi_{kl} u_l\right)\right\}\right] + \cdots \end{aligned} \qquad (i = 1, \cdots, n). \tag{35}$$

This solution is in general illusory on account of the divergence of certain series contained in the terms of the expansions formally representing the f's. In fact, let a_r and a_s be any two a's such that $|a_r| > |a_s|$. Put

$$C_i = 0, \ i \neq r; \qquad C_r = 1.$$

For $i = s$ the second term in the series in (35) becomes

$$\begin{aligned} S_{xs}(\phi_{sr} a_r^x x^{m_r}) &\equiv -\sum_{\nu=0}^{\infty} \frac{\phi_{sr}(x+\nu) a_r^{x+\nu} (x+\nu)^{m_r}}{\lambda_s(x) \cdots \lambda_s(x+\nu)} \\ &= -\sum_{\nu=0}^{\infty} \frac{\phi_{sr}(x+\nu) a_r^{x+\nu} (x+\nu)^{m_r}}{a_s^{x+\nu} (x+\nu)^{m_s}}, \end{aligned} \tag{36}$$

a series which is evidently divergent at least for some values of $\phi_{sr}(x)$ as for instance $\phi_{sr}(x) \equiv 1/x^2$.

On the other hand, there is at least one particular convergent solution, arising from the following special choice of values of the periodic functions C_i:

$$C_i = 0, \qquad i \neq 1; \qquad C_1 = 1.$$

If we call this particular solution $f_{i1}(x)$, we have formally from (35)

$$\begin{aligned} f_{i1}(x) = \delta_{i1} a_1^x x^{m_1} &+ S_{xi}(\phi_{i1} a_1^x x^{m_1}) + S_{xi}\left\{\sum_{j=1}^{n} \phi_{ij} S_{xj}(\phi_{j1} a_1^x x^{m_1})\right\} \\ &+ S_{xi}\left[\sum_{j=1}^{n} \phi_{ij} S_{xj}\left\{\sum_{k=1}^{n} \phi_{jk} S_{xk}(\phi_{k1} a_1^x x^{m_1})\right\}\right] + \cdots \quad (i = 1, \cdots, n). \end{aligned} \tag{37}$$

That all the infinite series contained in (37) are actually convergent in D_1 is readily shown. Consider the series

$$\delta_{i1}a_1^r x^{m_1} + \bar{S}_{ri}\left(\frac{Mc}{nx^2}a_1^r x^{m_1}\right) + \bar{S}_{ri}\left\{\frac{Mc}{nx^2}\sum_{j=1}^{n}\bar{S}_{rj}\left(\frac{Mc}{nx^2}a_1^r x^{m_1}\right)\right\} + \bar{S}_{ri}\left[\frac{Mc}{nx^2}\sum_{j=1}^{n}\bar{S}_{rj}\left\{\frac{Mc}{nx^2}\sum_{k=1}^{n}\bar{S}_{rk}\left(\frac{Mc}{nx^2}a_1^r x^{m_1}\right)\right\}\right] + \cdots, \tag{38}$$

where $\bar{S}_{ri}$ denotes what S_{ri} becomes when the terms of the series which it indicates are replaced by their absolute values. On account of the first inequality (30) it is evident that all the infinite series in (37) are convergent provided that all those in (38) are likewise convergent; for if these expansions are written out in detail, the former, term by term, is less in absolute value than the latter.

Compare (38) with the following series

$$a_1^r x^{m_1} + \bar{S}_{r1}\left(\frac{Mc}{x^2}a_1^r x^{m_1}\right) + \bar{S}_{r1}\left\{\frac{Mc}{x^2}\bar{S}_{r1}\left(\frac{Mc}{x^2}a_1^r x^{m_1}\right)\right\} + \bar{S}_{r1}\left[\frac{Mc}{x^2}\bar{S}_{r1}\left\{\frac{Mc}{x^2}\bar{S}_{r1}\left(\frac{Mc}{x^2}a_1^r x^{m_1}\right)\right\}\right] + \cdots. \tag{39}$$

On account of inequality (31) it is clear that the convergence of (39) carries with it the convergence of (38); this is at once apparent from a term by term comparison of the two series, since (39) is obtained from (38) by replacing each denominator by one at least as great. But (39) (except for its first term) is of the same form as the series in the first members of (15) and (19). Hence, just as in the case of the latter series, one proves that throughout the region D_1 the successive terms of (38) represent analytic functions and finally that the series itself represents an analytic function.

We shall now find an upper bound for the values of the $n-1$ functions $f_{i1}(x)$, $i=2, \cdots, n$, as x varies within P_1; and, for similar variation of x, both upper and lower bounds for the values of $f_{11}(x)$. We have evidently

$$f_{i1}(x) < \bar{S}_{r1}\left(\frac{Mc}{x^2}a_1^r x^{m_1}\right) + \bar{S}_{r1}\left\{\frac{Mc}{x^2}\bar{S}_{r1}\left(\frac{Mc}{x^2}a_1^r x^{m_1}\right)\right\} + \cdots < |a_1^r x^{m_1}|\left\{\frac{M}{u-1} + \frac{M^2}{(u-1)^2} + \cdots\right\} \qquad (i=2, \cdots, n),$$

the latter inequality being deduced by aid of (15). Hence it is clear that

$$|f_{i1}(x)| < |a_1^r x^{m_1}|\frac{M}{u-M-1} \qquad (i=2, \cdots, n). \tag{40}$$

Similarly, one has

$$|f_{11}(x)| < |a_1^r x^{m_1}|\left(1 + \frac{M}{u-M-1}\right) = |a_1^r x^{m_1}|\frac{u-1}{u-M-1};$$

and also,

$$|f_{i1}(x)| > |a_1^x x^{m_1}| \left(1 - \frac{M}{u-M-1}\right) = |a_1^x x^{m_1}| \frac{u-2M-1}{u-M-1}.$$

Combining these two inequalities we get

$$|a_1^x x^{m_1}| \frac{u-2M-1}{u-M-1} < |f_{i1}(x)| < |a_1^x x^{m_1}| \frac{u-1}{u-M-1}. \tag{41}$$

The desired results for the region P_1 are contained in inequalities (40) and (41).

Starting from (19) and working in a similar manner one obtains the following inequalities valid in Q_1:

$$|f_{i1}(x)| < |a_1^x x^{m_1}| \frac{A}{v-A} \qquad (i=2, \cdots, n); \tag{42}$$

$$|a_1^x x^{m_1}| \frac{v-2A}{v-A} < |f_{i1}(x)| < |a_1^x x^{m_1}| \frac{v}{v-A}. \tag{43}$$

By means of (27) we are able to determine the nature of $f_{i1}(x)$, $i=1, \cdots, n$, in the region E_1; for we have

$$f_{i1}(x-1) = \sum_{j=1}^{n} \bar{\psi}_{ij}(x-1) f_{j1}(x). \tag{44}$$

Now the functions $f_{i1}(x)$ are analytic throughout P_1. This solution may therefore be extended across the plane to the left by means of (44); it is evident from the nature of the process that the singularities of $f_{i1}(x)$ for x in E_1 are at the singularities of $\bar{\psi}_{ij}(x)$, $i, j=1, \cdots, n$, and the points congruent to them on the left. The nature of the singularities which the functions $f_{i1}(x)$ may have depends upon the particular functions $\bar{\psi}_{ij}(x)$ entering into a given particular system of equations. In special cases it may happen that some or all of the functions have no singularities at the points indicated.

Inequalities bounding the increase or decrease of $|f_{i1}(x)|$ for x in E_1 are not as complete as those for x in P_1 and Q_1. We shall however obtain bounds for $|f_{i1}(x)|$ when x is in $E_{1\epsilon}$, $E_{1\epsilon}$ being defined as follows: Let $[S]$ be the set of points composed of all the singularities of $\bar{\psi}_{ij}(x)$, $i, j=1, \cdots, n$, and the points congruent to them on the left. Enclose each point of $[S]$ by a circle of radius ϵ having the point for center. The part of E_1 no point of which is interior to one of these circles is the region $E_{1\epsilon}$.

Referring to the definition of $\bar{\psi}_{ij}(x)$ in equation (28), it is easy to see that

$$\lim_{x=\infty} \alpha_{ij}(x) = \begin{cases} 0 \text{ if } j \neq i, \\ a_i^{-1} \prod_{s=1}^{n} a_s \text{ if } j = i, \end{cases}$$

and that

$$\underset{x=\infty}{L}\,\Delta = \prod_{s=1}^{n} a_s .$$

Hence we have

$$\underset{x=\infty}{L}\,\bar{\psi}_{ij}(x) = \begin{cases} 0 \text{ if } j \neq i, \\ a_i^{-1} \text{ if } j = i. \end{cases}$$

From this it follows that for every positive constant a such that $a < |a_1|$ there exists a positive constant r for which

$$\sum_{j=1}^{n} |\bar{\psi}_{ij}(x)| < a^{-1} \qquad (i = 1, \cdots, n) \qquad |x| \geqq r.$$

It will be assumed that r is so taken that the circle $|x| = r$ cuts the boundary of E_1 in two points on the left of the origin and in no other point.

Since each of the functions $f_{i1}(x)$ is analytic throughout E_{1e} it follows that a constant $\bar{N}$ exists such that

$$|f_{i1}(x'')| < \bar{N} \text{ for } x'' \text{ in } E_{1e} \text{ and } r \leqq |x''| \leqq r + 1.$$

But from (27) we have

$$f_{i1}(x'' - \mu) = \sum_{j_1=1}^{n} \bar{\psi}_{ij_1}(x'' - \mu) \sum_{j_2=1}^{n} \bar{\psi}_{j_1 j_2}(x'' - \mu + 1) \cdots \sum_{j_\mu=1}^{n} \bar{\psi}_{j_{\mu-1} j_\mu}(x'' - 1) f_{j_\mu 1}(x'').$$

Hence we get

$$|f_{i1}(x'' - \mu)| < \bar{N} a^{-\mu}.$$

As μ varies over the range $\mu = 0, 1, 2, \cdots, x'' - \mu$ runs over all points in E_{1e} and outside of the circle $|x| = r$. Also, $|f_{i1}(x)|$ is finite in the part of E_{1e} which is in the circle $|x| = r$. Hence it is clear that there exists a constant N, such that

$$|f_{i1}(x)| < N|a^x| \qquad (i = 1, \cdots, n) \qquad x \text{ in } E_{1e}.$$

The principal results of the section may be stated as follows:

The system of difference equations

$$f_i(x+1) = \sum_{j=1}^{n} \psi_{ij}(x) f_j(x) \quad \text{or} \quad f_i(x-1) = \sum_{j=1}^{n} \bar{\psi}_{ij}(x-1) f_j(x) \quad (i = 1, \cdots, n),$$

in which $\psi_{ij}(x)$ is single-valued and

$$\psi_{ij}(x) = \delta_{ij} a_i \left(1 + \frac{1}{x}\right)^{m_i} + \phi_{ij}(x), \qquad \phi_{ij}(x) = \phi''_{ij} x^{-2} + \phi'''_{ij} x^{-3} + \cdots$$

for $|x| \geqq R > 1$,

$$\delta_{ij} = 0 \text{ when } i \neq j; \qquad \delta_{ii} = 1,$$

has a particular solution, $f_{i1}(x)$, each function of which is analytic throughout the finite plane except at the singularities $[\alpha]$ of $\bar{\psi}_{ij}(x)$ and the points con-

gruent to them on the left. If D_1 is defined by relations (30) *to* (34), *then throughout any closed region in D_1 this solution is representable as a uniformly converging series in the form*

$$f_{i1}(x) = \delta_{i1} a_1^r x^{m_1} + S_{ri}(\phi_{i1} a_1^r x^{m_1}) + S_{ri}\left\{\sum_{j=1}^{n} \phi_{ij}\, S_{rj}(\phi_{j1} a_1^r x^{m_1})\right\}$$

$$+ S_{ri}\left[\sum_{j=1}^{n} \phi_{ij}\, S_{rj}\left\{\sum_{k=1}^{n} \phi_{jk} S_{rk}(\phi_{k1} a_1^r x^{m_1})\right\}\right] + \cdots \quad (i = 1, \cdots, n).$$

The increase or decrease of these functions for x in the corresponding regions P_1 and Q_1 is bounded as in the inequalities

$$|a_1^r x^{m_1}| \frac{u - 2M - 1}{u - M - 1} < |f_{11}(x)| < |a_1^r x^{m_1}| \frac{u - 1}{u - M - 1}, \quad \textit{for } x \textit{ in } P_1;$$

$$|a_1^r x^{m_1}| \frac{v - A}{v - 2A} < |f_{11}(x)| < |a_1^r x^{m_1}| \frac{v}{v - A}, \quad \textit{for } x \textit{ in } Q_1;$$

$$|f_{i1}(x)| < |a_1^r x^{m_1}| \frac{M}{u - M - 1} \qquad (i = 2, \cdots, n), \quad \textit{for } x \textit{ in } P_1;$$

$$|f_{i1}(x)| < |a_1^r x^{m_1}| \frac{A}{v - A} \qquad (i = 2, \cdots, n), \quad \textit{for } x \textit{ in } Q_1.$$

Moreover for any positive constant a such that $a < |a_1|$ there exists another constant N such that

$$|f_{i1}(x)| < N|a^r| \qquad (i = 1, \cdots, n), \quad \textit{for } x \textit{ in } E_{1a}.$$

REMARK. It is important for later use to point out the fact that, in so far as any statement in the conclusion of the theorem refers to the region D_1 or any part of it, it is independent of the nature of $\phi_{ij}(x)$, $i, j = 1, \cdots, n$, in the region exterior to D_1. Hence, *if the functions $\phi_{ij}(x)$ are analytic in some D-region and satisfy the inequalities*

$$|\phi_{ij}(x)| < \frac{Mc}{n|x|^2} \qquad (i, j = 1, \cdots, n), \quad \textit{for } x \textit{ in } D, \tag{45}$$

then there exists a region D_1 having properties as in the theorem, and the system of equations has a particular solution $f_{i1}(x)$ having in D_1 the properties of $f_{i1}(x)$ of the theorem.

§ 3. *Existence of n independent solutions of the normal system.*

For the system of equations considered in the preceding section we shall now obtain n particular solutions which are independent and therefore constitute a fundamental system of solutions.

Since by (37) it is seen that $f_{11}(x)$ is not identically zero, we may make the substitution

$$g_1(x) = f_1(x), \tag{46}$$

$$g_i(x) = f_i(x) - \frac{f_{i1}(x)}{f_{11}(x)} f_1(x) \qquad (i = 2, \cdots, n), \tag{47}$$

of which the inverse is

$$f_1(x) = g_1(x), \qquad f_i(x) = \frac{f_{i1}(x)}{f_{11}(x)} g_1(x) + g_i(x) \quad (i = 2, \cdots, n), \tag{48}$$

where $f_{i1}(x)$, $i = 1, \cdots, n$, is the solution of (24) obtained in the preceding section. Then we have

$$\begin{aligned} g_i(x+1) &= f_i(x+1) - \frac{f_{i1}(x+1)}{f_{11}(x+1)} f_1(x+1) \\ &= \sum_{j=1}^{n} \left\{ \psi_{ij}(x) - \frac{f_{i1}(x+1)}{f_{11}(x+1)} \psi_{1j}(x) \right\} f_j(x) \end{aligned} \qquad (i = 2, \cdots, n).$$

Substituting in this equation the value of $f_j(x)$ obtained from (48) we have

$$\begin{aligned} g_i(x+1) &= \sum_{j=2}^{n} \left\{ \psi_{ij}(x) - \frac{f_{i1}(x+1)}{f_{11}(x+1)} \psi_{1j}(x) \right\} g_j(x) \\ &\quad + f_1(x) \sum_{j=1}^{n} \left\{ \psi_{ij}(x) - \frac{f_{i1}(x+1)}{f_{11}(x+1)} \psi_{1j}(x) \right\} \frac{f_{j1}(x)}{f_{11}(x)} \end{aligned} \qquad (i = 2, \cdots, n). \tag{49}$$

The last line of the expression may be written in the form

$$\frac{g_1(x)}{f_{11}(x)} \left\{ \sum_{j=1}^{n} \psi_{ij}(x) f_{j1}(x) - \frac{f_{i1}(x+1)}{f_{11}(x+1)} \sum_{j=1}^{n} \psi_{1j}(x) f_{j1}(x) \right\}.$$

Since $f_{j1}(x)$, $j = 1, \cdots, n$, is a solution of (24), this reduces to

$$\frac{g_1(x)}{f_{11}(x)} \left\{ f_{i1}(x+1) - \frac{f_{i1}(x+1)}{f_{11}(x+1)} f_{11}(x+1) \right\},$$

an expression which is identically zero. Hence in writing (49) the last line may be omitted. Thus we have

$$g_i(x+1) = \sum_{j=2}^{n} \left\{ \psi_{ij}(x) - \frac{f_{i1}(x+1)}{f_{11}(x+1)} \psi_{1j}(x) \right\} g_j(x) \quad (i = 2, \cdots, n). \tag{50}$$

Substituting the values of $f_i(x)$, $i = 1, \cdots, n$, obtained from (48) in the first equation of system (24), we have

$$g_1(x+1) = \sum_{j=1}^{n} \frac{f_{j1}(x)}{f_{11}(x)} \psi_{1j}(x) g_1(x) + \sum_{j=2}^{n} \psi_{1j}(x) g_j(x). \tag{51}$$

Replacing in (51) and (50) the functions $\psi_{ij}(x)$ by their original values, we

obtain the transformed system of equations:

$$(52)\quad g_1(x+1)-a_1\left(1+\frac{1}{x}\right)^{m_1}g_1(x)=\sum_{j=1}^{n}\frac{f_{j1}(x)}{f_{11}(x)}\phi_{1j}(x)g_1(x)+\sum_{j=2}^{n}\phi_{1j}(x)g_j(x),$$

$$(53)\quad g_i(x+1)-a_i\left(1+\frac{1}{x}\right)^{m_i}g_i(x)=\sum_{j=2}^{n}\left\{\phi_{ij}(x)-\frac{f_{i1}(x+1)}{f_{11}(x+1)}\phi_{1j}(x)\right\}g_j(x)$$
$$(i=2,\cdots,n).$$

This system has the simple solution

$$g_1(x)=f_{11}(x),\qquad g_i(x)=0\qquad (i=2,\cdots,n).$$

By substitution of this solution in (48) one reproduces of course the known solution of (24). We shall prove next that system (52), (53) has a second solution, and by means of it find a second solution of (24).

It will be noticed that the $n-1$ equations (53) involve only the $n-1$ functions $g_i(x)$, $i=2,\cdots,n$; and therefore (53) is a system of $n-1$ equations in these unknowns. It satisfies the hypotheses of the theorem indicated in the remark at the close of § 2; that is, there exist a constant M' ($\geqq M$) and a D-region such that each of the coefficient functions

$$\phi_{ij}(x)-\frac{f_{i1}(x+1)}{f_{11}(x+1)}\phi_{1j}(x)\qquad (i,j=2,\cdots,n),$$

is analytic in D and the inequality

$$\left|\phi_{ij}(x)-\frac{f_{i1}(x+1)}{f_{11}(x+1)}\phi_{1j}(x)\right|<\frac{M'c}{(n-1)|x|^2}$$

is satisfied by every x in D. The statement referring to the analytic nature of the coefficients is evidently true; for in a suitable D-region $f_{11}(x)$ does not vanish. It is clear also that there exists a constant M' such that the above inequality is true provided that there is a D-region in which $f_{i1}(x+1)/f_{11}(x+1)$ is in absolute value equal to or less than 1. That this is true follows at once from inequalities (40) to (43).

From the above considerations and the theorem indicated in the remark referred to may be drawn several conclusions which are important for the succeeding argument:

1) There exist particular regions P_2, Q_2, D_2 and constants c and $M_1(\geqq M')$ such that inequalities analogous to (30) to (34) hold and such that also

$$(54)\quad u>2M_1+1,\qquad A_1/v<\tfrac{1}{2},\qquad |f_{i1}(x)/f_{11}(x)|\leqq 1,\quad \text{for } x \text{ in } D_2.$$

2) The system of equations (53) has a particular solution, $g_{i2}(x)$, $i=2,\cdots,n$, each function of which is analytic throughout D_2.

3) The increase or decrease of the functions which constitute this solution is

bounded as follows:

$$
\begin{aligned}
&|a_2^x x^{m_2}|\frac{v-2A_1}{v-A_1}<|g_{22}(x)|<|a_2^x x^{m_2}|\frac{v}{v-A_1},\\
&|g_{i2}(x)|<|a_2^x x^{m_2}|\frac{A_1}{v-A_1}\quad (i=3,\cdots,n),
\end{aligned}
\tag{55}
$$

for x in Q_2;

$$
\begin{aligned}
&|a_2^x x^{m_2}|\frac{u-2M_1-1}{u-M_1-1}<|g_{22}(x)|<|a_2^x x^{m_2}|\frac{u-1}{u-M_1-1},\\
&|g_{i2}(x)|<|a_2^x x^{m_2}|\frac{M_1}{u-M_1-1}\quad (i=3,\cdots,n),
\end{aligned}
\tag{56}
$$

for x in P_2.

These $n-1$ functions are a part of a particular solution of the system (52), (53). To find the other function $g_{12}(x)$ of this solution we have the non-homogeneous equation

$$
\begin{aligned}
&g_{12}(x+1)-a_1\left(1+\frac{1}{x}\right)^{m_1}g_{12}(x)\\
&\qquad=\sum_{j=1}^{n}\frac{f_{j1}(x)}{f_{11}(x)}\phi_{1j}(x)g_{12}(x)+\sum_{j=2}^{n}\phi_{1j}(x)g_{j2}(x).
\end{aligned}
\tag{57}
$$

We obtain first a solution of the reduced equation

$$
g(x+1)-a_1\left(1+\frac{1}{x}\right)^{m_1}g(x)=\sum_{j=1}^{n}\frac{f_{j1}(x)}{f_{11}(x)}\phi_{1j}(x)g(x),
\tag{58}
$$

an equation which satisfies the hypotheses of the theorem indicated in the remark at the close of § 1, as is shown by relations (54) and those indicated in the lines preceding (54). Accordingly it has a particular solution $\bar{g}(x)$ analytic and not zero throughout D_2 and approximately characterized by the inequalities

$$
\begin{aligned}
&|a_1^x x^{m_1}|\frac{v-2A_1}{v-A_1}<|\bar{g}(x)|<|a_1^x x^{m_1}|\frac{v}{v-A_1},\quad \text{for } x \text{ in } Q_2;\\
&|a_1^x x^{m_1}|\frac{u-2M_1-1}{u-M_1-1}<|\bar{g}(x)|<|a_1^x x^{m_1}|\frac{u-1}{u-M_1-1},\quad \text{for } x \text{ in } P_2.
\end{aligned}
\tag{59}
$$

Substituting in (57)

$$
g_{12}(x)=h(x)\bar{g}(x)
\tag{60}
$$

and making use of the fact that $\bar{g}(x)$ satisfies (58), one obtains by easy reduction

$$
h(x+1)-h(x)=\sum_{j=2}^{n}\frac{\phi_{1j}(x)g_{j2}(x)}{\bar{g}(x+1)}=\eta(x).
\tag{61}
$$

It is clear that $\eta(x)$ is analytic throughout D_2.

Bounds of increase or decrease of $\eta(x)$ may be readily obtained. From (55),

(56), and (59) we have

$$(62)\qquad \begin{aligned} |\eta(x)| &< \left|\left(\frac{a_2}{a_1}\right)^x x^{m_2-m_1-2}\right| \frac{Mv}{v-2A_1}, \quad \text{for } x \text{ in } Q_2; \\ |\eta(x)| &< \left|\left(\frac{a_2}{a_1}\right)^x x^{m_2-m_1-2}\right| \frac{M(u-1)}{u-2M_1-1}, \quad \text{for } x \text{ in } P_2. \end{aligned}$$

From the first of these inequalities it is clear that the series

$$(63)\qquad s(x) = \eta(x-1) + \eta(x-2) + \eta(x-3) + \cdots$$

is uniformly convergent throughout any closed region in Q_2; and hence the function $s(x)$ is analytic in Q_2. We have also

$$(64)\qquad s(x+1) - s(x) = \eta(x),$$

so that $h(x) = s(x)$ is a solution of (61) which is analytic in Q_2. But its behavior near the positive real axis is complicated; and the solution of (52), (53), and hence of (24), to which it leads is composed of functions which are complicated in their character in the same region. We seek therefore another solution, one which will avoid this difficulty near the real axis; it will of course differ from $s(x)$ by a periodic function.

A solution of (61) in the form of a contour integral, the path of integration going to infinity along two parallel lines, will be found to serve our purpose. We form the integral

$$(65)\qquad I(x) = \int_L \frac{\eta(z)\,dz}{1 - e^{2\pi i(x-z)}},$$

where the path of integration L is yet to be chosen. Since $\eta(x)$ is analytic throughout D_2, it is evident that all the infinities which the integrand has in D_2 are at the points $x \pm r$, where r is zero or a positive integer. Let AB be the straight line containing all these points. Let the path of integration L or $CKRH$ lie entirely in D_2 and be formed in the following manner: It consists

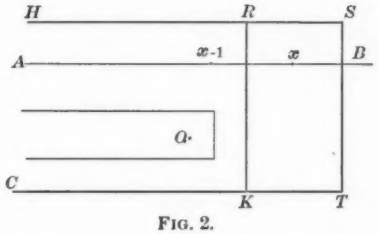

FIG. 2.

of three parts: a part RH lying entirely above AB and extending to infinity in a negative direction parallel to the axis of reals; a part KC lying below AB and

extending to infinity in a negative direction parallel to the axis of reals; a finite part KR which crosses AB once between $x-1$ and x and at no other point. Moreover the path $CKRH$ is such that E_2 lies entirely to the left of it. From (62) it is evident that the integral along such a path has a meaning. It is clear that for a particular x the path of integration may be deformed at will without changing the value of $I(x)$, provided that during the deformation it has always the properties stated in the definition of $CKRH$. Furthermore, $I(x)$ is analytic in D_2.

We show that $h(x) = I(x)$ is a solution of (61). In view of the fact that the integrand considered as a function of x is periodic of period 1 it is clear that we have

$$I(x+1) = \int_{L'} \frac{\eta(z)\,dz}{1-e^{2\pi i(x-z)}}, \tag{66}$$

where L' is the path $CTSH$. Now

$$\int_{L'} - \int_{L} = \int_{KTSRK}.$$

But by Cauchy's theorem the last integral is equal to $\eta(x)$. Hence, subtracting (65) from (66), member by member, we have

$$I(x+1) - I(x) = \eta(x);$$

that is,

$$h(x) = I(x)$$

is a solution of (61). It is this particular solution which we shall take for the value of $h(x)$ in the remaining discussion. It is analytic in D_2, as we have seen.

It is necessary, for later use, to know a bound to the increase or decrease of $|h(x)|$ for x in Q_2 and P_2. We consider the two regions separately, first taking the region Q_2. On account of (64) and the analytic nature of both $h(x)$ and $s(x)$ in Q_2, it is evident that $h(x) - s(x)$ is a periodic function of x of period 1 and analytic throughout Q_2. Now

$$|h(x)| \leqq |h(x) - s(x)| + |s(x)|; \tag{67}$$

accordingly we find upper bounds for $|h(x) - s(x)|$ and $|s(x)|$ separately. Consider the function $h(x) - s(x)$ for $x = u \pm v\sqrt{-1}$, x being in Q_2, where v is fixed and where u runs over any stretch of length 1. For such variation of x, $|h(x) - s(x)|$ has evidently a maximum which is entirely independent of the range for u but depends directly on v. Call this maximum $m(\pm v)$. Then we have

$$|h(x) - s(x)| \leqq m(\pm v), \quad \text{for } x \text{ in } Q_2, \tag{68}$$

where $m(\pm v)$ is a single-valued function of $\pm v$.

Now

$$|s(x)| \leqq \sum_{i=1}^{\infty} |\eta(x-i)| < \frac{Mv}{v-2A_1} \sum_{i=1}^{\infty} \left|\left(\frac{a_2}{a_1}\right)^{x-i} (x-i)^{m_2-m_1-2}\right|,$$

by (62). Hence we have

$$|s(x)| < \frac{Mv}{v-2A_1} \left|\left(\frac{a_2}{a_1}\right)^{x} x^{m_2-m_1-2} \sum_{i=1}^{\infty} \left(\frac{a_1}{a_2}\right)^{i} \left(1-\frac{i}{x}\right)^{m_2-m_1-2}\right|.$$

Therefore we obtain the result

$$|s(x)| < \frac{B_1}{|x|^2} \left|\left(\frac{a_2}{a_1}\right)^{x} x^{m_2-m_1}\right|, \quad \text{for } x \text{ in } Q_2, \tag{69}$$

where B_1 is a properly chosen constant. Then, finally, from (67), (68), (69) we have

$$|h(x)| < m(\pm v) + \frac{B_1}{|x|^2} \left|\left(\frac{a_2}{a_1}\right)^{x} x^{m_2-m_1}\right|, \quad \text{for } x \text{ in } Q_2. \tag{70}$$

In order to find an upper bound for $|h(x)|$ when x is in P_2 we proceed as follows: Let AB be the line parallel to the axis of reals and containing the

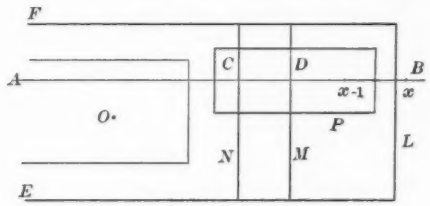

FIG. 3.

point x. Construct the contours ELF, EMF, ENF, P as in the figure, where the stretch CD is equal to $\frac{1}{2}$. Let us denote by $I_L(x)$, $I_M(x)$, $I_N(x)$, $I_P(x)$ respectively the integral

$$\int \frac{\eta(z)\,dz}{1-e^{2\pi i(x-z)}}$$

taken around these contours. For any value of x, either $I_M(x)$ or $I_N(x)$ represents an integral which is convergent, though the path of integration of one of them may pass through an infinity of the integrand. $I_L(x)$ and $I_P(x)$ always have a meaning, if it is understood that the contour P may vary so as not to cross AB at a point congruent to x.

Since $h(x) \equiv I_L(x)$, we clearly have

$$\begin{aligned} |h(x)| &\leqq |I_M(x)| + \bar{I}_P(x), \\ |h(x)| &\leqq |I_N(x)| + \bar{I}_P(x), \end{aligned} \quad \text{for } x \text{ in } P_2,$$

where $\bar{I}_P(x)$ is the quantity obtained by applying to $I_P(x)$ the calculus of residues and replacing by its absolute value each term of the sum so obtained. Let x vary along AB. For each x take the smaller of the quantities $|I_M(x)|$ and $|I_N(x)|$; call this quantity $\tau(x)$. From the nature of the integrand in $I(x)$, it is evident that $\tau(x)$ has a maximum; we denote this maximum by $\mu(\pm v)$, since it depends on $\pm v$ alone. Thus we obtain

$$|h(x)| \leqq \mu(\pm v) + \bar{I}_P(x), \quad \text{for } x \text{ in } P_2.$$

Now from (62) and the calculus of residues it is clear that when x is in P_2 we have

$$|I_P(x)| < \frac{M(u-1)}{u-2M_1-1} \sum_{i=1}^{\infty} \left| \left(\frac{a_2}{a_1}\right)^{x-i} (x-i)^{m_2-m_1-2} \right|.$$

Hence we obtain

$$|I_P(x)| < \frac{B_2}{|x|^2} \left| \left(\frac{a_2}{a_1}\right)^{x} x^{m_2-m_1} \right|, \quad \text{for } x \text{ in } P_2,$$

where B_2 is a properly chosen constant. Therefore we have

$$(\overline{70}) \qquad |h(x)| < \mu(\pm v) + \frac{B_2}{|x|^2} \left| \left(\frac{a_2}{a_1}\right)^{x} x^{m_2-m_1} \right|, \quad \text{for } x \text{ in } P_2.$$

Since $h(x)$ and $\bar{g}(x)$ are known functions, both analytic throughout D_2, equation (60) gives us a function $g_{12}(x)$ analytic in D_2. From (59), (70), ($\overline{70}$) we have

$$(71) \quad \begin{cases} |g_{12}(x)| < |a_1^x x^{m_1}| \dfrac{v \cdot m(\pm v)}{v - A_1} + |a_2^x x^{m_2}| \dfrac{B_2}{|x|^2} \cdot \dfrac{v}{v - A_1}, & \text{for } x \text{ in } Q_2; \\ |g_{12}(x)| < |a_1^x x^{m_1}| \dfrac{\mu(\pm v)(u-1)}{u-M_1-1} + |a_2^x x^{m_2}| \dfrac{B_2}{|x|^2} \cdot \dfrac{u-1}{u-M_1-1}, & \text{for } x \text{ in } P_2. \end{cases}$$

From (48) we now have a second solution of (24); calling it $f_{i2}(x)$, $i = 1, \cdots, n$, we may write

$$(72) \quad \begin{cases} f_{12}(x) = g_{12}(x), \\ f_{i2}(x) = \dfrac{f_{i1}(x)}{f_{11}(x)} g_{12}(x) + g_{i2}(x) & (i = 2, \cdots, n). \end{cases}$$

Also from (55), (56), (71) we have the following inequalities:

$$(73) \quad \begin{cases} |f_{12}(x)| < |a_2^x x^{m_2}| \dfrac{B_2}{|x|^2} \cdot \dfrac{v}{v - A_1} + |a_1^x x^{m_1}| \dfrac{v \cdot m(\pm v)}{v - A_1}, \\ |f_{22}(x)| < |a_2^x x^{m_2}| \dfrac{v}{v - A_1} + |f_{12}(x)|, \\ |f_{22}(x)| > |a_2^x x^{m_2}| \dfrac{v - 2A_1}{v - A_1} - |f_{12}(x)|, \\ |f_{i2}(x)| < |a_2^x x^{m_2}| \dfrac{A_1}{v - A_1} + |f_{12}(x)| \quad (i = 3, \cdots, n), \end{cases} \qquad \text{for } x \text{ in } Q_2;$$

$$(74)\quad \begin{cases} |f_{12}(x)| < |a_2^x x^{m_2}| \dfrac{B_2}{|x|^2} \cdot \dfrac{u-1}{u-M_1-1} + |a_1^x x^{m_1}| \dfrac{\mu(\pm v)(u-1)}{u-M_1-1}, \\ |f_{22}(x)| < |a_2^x x^{m_2}| \dfrac{u-1}{u-M_1-1} + |f_{12}(x)|, \\ |f_{22}(x)| > |a_2^x x^{m_2}| \dfrac{u-2M_1-1}{u-M_1-1} - |f_{12}(x)|, \\ |f_{i2}(x)| < |a_2^x x^{m_2}| \dfrac{M_1}{u-M_1-1} + |f_{12}(x)| \quad (i=3, \cdots, n), \end{cases} \qquad \text{for } x \text{ in } P_2.$$

It should be observed that the results of this paragraph, inasmuch as they refer only to the region D_2, are again independent of the nature of the functions $\phi_{ij}(x)$ in E_2.

If $n > 2$ we may obtain a third solution of (24) in the following manner: The solution of (24) just obtained depends intimately upon the two smallest a's in the system, as inequalities (73), (74) show. Hence it follows that (53) has a corresponding solution depending in like manner upon the two smallest a's in that system; this solution we shall call $g_{i3}(x)$, $i = 2, \cdots, n$. It is analytic throughout some region D_3 and satisfies the inequalities corresponding to (73):

$$(75)\quad \begin{cases} |g_{23}(x)| < |a_3^x x^{m_3}| \dfrac{B_3}{|x|^2} \cdot \dfrac{v}{v-A_2} + |a_2^x x^{m_2}| \dfrac{v \cdot m_1(\pm v)}{v-A_2}, \\ |g_{33}(x)| < |a_3^x x^{m_3}| \dfrac{v}{v-A_2} + |g_{23}(x)|, \\ |g_{33}(x)| > |a_3^x x^{m_3}| \dfrac{v-2A_2}{v-A_2} - |g_{23}(x)|, \\ |g_{i3}(x)| < |a_3^x x^{m_3}| \dfrac{A_2}{v-A_2} + |g_{23}(x)| \quad (i=4, \cdots, n), \end{cases} \qquad \text{for } x \text{ in } Q_3;$$

where D_3, Q_3, $m_1(\pm v)$, A_2, B_3 are defined in a manner analogous respectively to the definitions of D_2, Q_2, $m(\pm v)$, A_1, B_1. Also there exists of course a set of inequalities similar to (74) for x in P_3; it is not necessary to write them out.

We have thus $n-1$ functions of a third solution of (52), (53). To find the other function, which we will call $g_{13}(x)$, we have an equation corresponding to (57) above. If we write

$$g_{13}(x) = h_1(x)\bar{g}(x),$$

where $\bar{g}(x)$ is defined as before, it is easy to see that $h_1(x)$ is a solution of

$$(76)\qquad h_1(x+1) - h_1(x) = \sum_{j=2}^{n} \frac{\phi_{1j}(x) g_{j3}(x)}{\bar{g}(x+1)} \equiv \eta_1(x).$$

From inequalities (59), (75) and those for x in P_3 corresponding to (75) and the fact that $\eta_1(x)$ is analytic throughout D_3 it follows that the method used for solving (61) is applicable to (76) and that a solution may be obtained as before in the form of a contour integral. We thus find a third particular solution of (52), (53). Just as before this leads to a solution of (24). It is evident that this process may be continued until n particular solutions of (24) are obtained and that there exists a D-region in which each of the n^2 functions of these solutions is analytic. We shall call these n solutions

$$f_{1j}(x),\ f_{2j}(x),\ \cdots,\ f_{nj}(x) \qquad (j=1,\cdots,n). \tag{77}$$

It is clear that we may employ (27) to extend each of these solutions across the plane to the left and in this way prove that each function $f_{ij}(x)$ is analytic throughout the finite plane except at the singularities of $\bar{\psi}_{ij}(x)$ and the points congruent to them on the left.

A reference to the discussion (in the preceding section) of the bounds of $|f_{ii}(x)|$ in the region E_1 will bring out the fact that an argument similar to that employed there is applicable to any one of the n particular solutions which we have obtained, and that the result in each case takes the same form as that obtained for the first solution.

Let us now write

$$f_{ij}(x) = a_j^x x^{m_j} U_{ij}(x) \qquad (i,j=1,\cdots,n),$$

where the functions $U_{ij}(x)$ are defined by these equations. Inequalities (40) to (43), (73), (74) and the analogous inequalities for the other solutions enable us to conclude (without further argument) that when x approaches infinity in the positive direction along any line parallel to the real axis we have *

$$\lim U_{ij}(x) = \begin{cases} 0 \text{ if } i \neq j, \\ 1 \text{ if } i = j. \end{cases} \tag{78}$$

This fact will enable us to prove the independence of the solutions (77). The necessary and sufficient condition for such independence † is that the determinant of which $f_{ij}(x)$ is the general element is not identically zero. Now we have

$$|f_{ij}(x)| = a_1^x a_2^x \cdots a_n^x x^{m_1+m_2+\cdots+m_n} |U_{ij}(x)|.$$

From this result and (78) it follows that the determinant of which $f_{ij}(x)$ is the

* This result brings into prominent notice the important question of the asymptotic character of the solutions for every approach to infinity. The full discussion of this subject requires a separate investigation. There are several excellent papers by HORN, FORD, PERRON and others treating the highly important special case in which x runs over a set of points $x_0, x_0+1, x_0+2, \cdots$. See references on pp. 160, 190, 191 of HORN's paper in Crelle's Journal, vol. 138 (1910). To the papers which he lists should be added one by PERRON in Jahresbericht der deutschen Mathematiker-Vereinigung, vol. 19 (1910), pp. 129–137. See also the paper by WATSON referred to in the introduction to the present paper.

† Cf. PINCHERLE and AMALDI, *Le operazione distributive*, p. 218.

general element is not identically zero. Hence the solutions (77) are independent and form therefore a fundamental system of solutions of the system (24); and hence the general solution is

$$f_i(x) = \sum_{j=1}^{n} \omega_j(x) f_{ij}(x) \qquad (i = 1, \cdots, n),$$

where the functions $\omega_j(x)$, $j = 1, \cdots, n$, are arbitrary periodic functions of period 1.

In the theorem below, the inequalities bounding $|f_{ij}(x)|$, $i, j = 1, \cdots, n$, are not given; otherwise the principal results of the section are as follows:

The system of equations

$$f_i(x+1) = \sum_{j=1}^{n} \psi_{ij}(x) f_j(x) \quad \text{or} \quad f_i(x-1) = \sum_{j=1}^{n} \bar{\psi}_{ij}(x-1) f_j(x) \qquad (i = 1, \cdots, n),$$

$\psi_{ij}(x)$ being restricted as in the theorem of § 2, has the fundamental system of solutions

$$f_{1j}(x), f_{2j}(x), \cdots, f_{nj}(x) \qquad (j = 1, \cdots, n),$$

determined in the preceding pages and having the following properties: Each function $f_{ij}(x)$ is analytic throughout the finite plane except at the singularities of $\bar{\psi}_{ij}(x)$ and the points congruent to them on the left. The general solution of the system of equations is

$$f_i(x) = \sum_{j=1}^{n} \omega_j(x) f_{ij}(x) \qquad (i = 1, \cdots, n),$$

where the functions $\omega_j(x)$, $j = 1, \cdots, n$, are arbitrary periodic functions of period 1. Further, for x approaching infinity along any line parallel to the positive real axis we have

$$\lim f_{ij}(x) a_j^{-x} x^{-m_j} = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j. \end{cases}$$

§ 4. *Reduction to normal form. General existence theorems.*

Let

$$G_i(x+1) = x^{\alpha} \sum_{j=1}^{n} a_{ij}(x) G_j(x) \qquad (i = 1, \cdots, n), \tag{79}$$

be a system of n first order linear homogeneous difference equations involving n unknown functions $G_1(x), \cdots, G_n(x)$ of the complex variable x, the known quantities entering into the equation being defined as follows:

1) α is a constant;

2) the functions $a_{ij}(x)$ are single-valued and

$$a_{ij}(x) = a_{ij} + a'_{ij} x^{-1} + a''_{ij} x^{-2} + \cdots \qquad (i, j = 1, \cdots, n) \qquad |x| > R;$$

3) the constants a_{ij} are such that the roots of the equation

$$|a_{ij} - \delta_{ij}\rho| = 0, \qquad \delta_{ij} = \begin{cases} 0 \text{ if } i \neq j, \\ 1 \text{ if } i = j, \end{cases} \tag{80}$$

are in absolute value different from each other and from zero.

Equation (80) is the *characteristic equation* associated with (79). For convenience we assume that its roots $a_1, \cdots, a_n$ are arranged so that

$$0 < |a_1| < |a_2| < \cdots < |a_n|. \tag{81}$$

The object of this section is to extend the theorem of § 3 to the system in its more general form and then to apply the result to a single equation of the nth order. The work is carried out by first reducing (79) to the normal form already studied. In this discussion two properties of the Γ-function will be assumed; namely, that it is analytic to the right of the axis of imaginaries, and that it satisfies the functional equation

$$\Gamma(x+1) = x\Gamma(x). \tag{82}$$

It is obvious that α can be reduced to zero by means of the transformation

$$G_i(x) = \{\Gamma(x)\}^{\alpha}\bar{G}_i(x). \tag{83}$$

Effecting this substitution in (79) and reducing by means of (82) we have

$$\bar{G}_i(x+1) = \sum_{j=1}^{n} a_{ij}(x)\bar{G}_j(x) \qquad (i=1, \cdots, n). \tag{84}$$

The first step in the normalization of (84) will be made by means of a linear transformation with constant coefficients. This done, a further reduction (of a different type) will enable us to remove the term in x^{-1} from the resulting coefficient functions $\bar{a}_{ij}(x)$, $i \neq j$.

Let us put

$$\bar{G}_i(x) = \sum_{j=1}^{n} \alpha_{ij} F_j(x) \qquad (i=1, \cdots, n), \tag{85}$$

where the determinant $|\alpha_{ij}|$ is different from zero. Making this substitution in (84) and solving for $F_i(x+1)$ one may write the result in the form

$$F_i(x+1) = \sum_{j=1}^{n} \bar{a}_{ij}(x) F_j(x) \qquad (i=1, \cdots, n), \tag{86}$$

where the functions $\bar{a}_{ij}(x)$, being linear combinations of the functions $a_{ij}(x)$ with constant coefficients, may be expanded in powers of x^{-1} for $|x| > R'$.

In connection with this transformation, let us consider the effect in the linear substitution

$$y_i' = \sum_{j=1}^{n} a_{ij} y_j \qquad (i=1, \cdots, n), \tag{87}$$

of replacing y_i' and y_i by their values as given in the transformation

$$y_i = \sum_{j=1}^{n} \alpha_{ij} \bar{y}_j, \qquad y_i' = \sum_{j=1}^{n} \alpha_{ij} \bar{y}_j' \qquad (i = 1, \cdots, n). \tag{88}$$

Having made these substitutions, solve for $\bar{y}_i'$ and write the result

$$\bar{y}_i' = \sum_{j=1}^{n} \bar{a}_{ij} \bar{y}_j \qquad (i = 1, \cdots, n).$$

Comparing the operations of this paragraph with those of the preceding, it is easy to see that the constant term in the function $\bar{a}_{ij}(x)$ must be identical with $\bar{a}_{ij}$ for each pair of values i and j. But, on account of (81), it follows from the well-known theory* of linear substitutions that a proper determination of α_{ij} in (88) will transform (87) to the simpler system

$$\bar{y}_i' = a_i \bar{y}_i \qquad (i = 1, \cdots, n). \tag{89}$$

Suitable values of α_{ij} may be determined* by solving the following n systems of equations:

$$\sum_{j=1}^{n} a_{ij} \alpha_{j\tau} - a_\tau \alpha_{i\tau} = 0 \qquad (i, \tau = 1, \cdots, n), \tag{90}$$

a separate system being formed for each τ. That each system (90) is consistent follows from the fact that $\rho = a_\tau$ is a solution of the characteristic equation (80). Hence the ratios of $\alpha_{i\tau}$ for fixed τ and $i = 1, \cdots, n$ are determined by (90). Out of the infinity of proportional solutions of each of these n systems of equations we suppose a particular one chosen, and that the quantities α_{ij} have these fixed values throughout the remaining discussion.

If the values of α_{ij} so determined are used in (85), that transformation throws (84) into the simpler system

$$F_i(x+1) = a_i F_i(x) + \sum_{j=1}^{n} b_{ij}(x) F_j(x) \qquad (i = 1, \cdots, n), \tag{91}$$

where

$$b_{ij}(x) = b_{ij} x^{-1} + b_{ij}' x^{-2} + \cdots \qquad (i, j = 1, \cdots, n) \qquad |x| > R'.$$

In order to remove the term in x^{-1} from each of the coefficient functions $b_{ij}(x)$, $i \neq j$, we employ a transformation of the form

$$F_i(x) = f_i(x) + \sum_{j=1}^{n} \frac{\beta_{ij}}{x} f_j(x), \qquad \beta_{ii} = 0, \qquad (i = 1, \cdots, n), \tag{92}$$

where the constants β_{ij}, $i \neq j$, are as yet undetermined. The determinant of this transformation is

$$\Delta \equiv \left| \delta_{ij} + \frac{\beta_{ij}}{x} \right| = 1 + \text{terms in } x^{-2}, x^{-3}, \cdots.$$

*Cf. HORN, *Gewöhnliche Differentialgleichungen*, pp. 72–74.

Substituting these values for $F_i(x)$ in (91) and writing only those terms which do not involve $x^{-2}, x^{-3}, \cdots$, we have, when $|x| > R'$,

$$f_i(x+1) + \sum_{j=1}^{n}\left(\frac{\beta_{ij}}{x+1}\right) f_j(x+1) = a_i f_i(x) + a_i \sum_{j=1}^{n} \frac{\beta_{ij}}{x} f_j(x)$$

$$+ \sum_{j=1}^{n}\left\{\left(\frac{b_{ij}}{x} + \cdots\right)\left[f_j(x) + \sum_{k=1}^{n}\frac{\beta_{ik}}{x} f_k(x)\right]\right\} \tag{93}$$

$$= \left(a_i + \frac{b_{ii}}{x} + \cdots\right) f_i(x) + \sum_{j=1}^{n}{}' \left(\frac{a_i\beta_{ij} + b_{ij}}{x} + \cdots\right) f_j(x),$$

the accent in Σ' denoting that in the summation the term for which $j = i$ is to be omitted.

It is necessary to solve (93) for $f_i(x+1)$. We proceed thus: The cofactor Δ_{ij} of the element in the ith row and jth column of Δ has clearly no constant term, except when i equals j, when there is a constant term 1: the term in $1/x$ for $i \neq j$ is clearly $-\beta_{ji}/x$. For, if we cross out the ith row and jth column of Δ, there remain $n-2$ elements with a constant term 1; and therefore the expansion of this minor can contain only one term in $1/x$, namely that term which contains all the $n-2$ factors 1 and whose remaining factor is not in the same rows or columns as these. Therefore this term is $\pm\beta_{ji}/x$; and, since an even number of interchanges of rows and columns bring the elements β_{ij}/x and β_{ji}/x to the place in the first row second column and second row first column respectively, the negative sign must be chosen. In the cofactor Δ_{ii} there is no term in $1/x$; for every term in the expansion containing one factor $1/x$ necessarily contains another. Hence the cofactors may be written

$$\Delta_{ij} = -\frac{\beta_{ji}}{x} + \text{terms in } x^{-2}, x^{-3}, \cdots, \qquad (i \neq j);$$

$$\Delta_{ii} = 1 + \text{terms in } x^{-2}, x^{-3}, \cdots.$$

Solving (93) for $f_i(x+1)$ we readily obtain

$$\bar{\Delta} f_i(x+1) = \left(a_i + \frac{b_{ii}}{x} + \cdots\right) f_i(x) + \sum_{j=1}^{n}{}' \left\{\frac{(a_i - a_j)\beta_{ij} + b_{ij}}{x} + \cdots\right\} f_j(x) \tag{94}$$

$$(i = 1, \cdots, n),$$

$\bar{\Delta}$ denoting the determinant

$$\bar{\Delta} = \left|\delta_{ij} + \frac{\beta_{ij}}{x+1}\right|.$$

For values of x such that $|x| \geqq R''$, R'' being a properly chosen constant greater than R' and greater than 1, the determinant $\bar{\Delta}$ is everywhere different from zero and is expansible in the form 1 + terms in $x^{-2}, x^{-3}, \cdots$. If we divide by

$\bar{\Delta}$ we obtain therefore

$$(95)\quad f_i(x+1)=\left(a_i+\frac{b_{ii}}{x}+\cdots\right)f_i(x)+\sum_{j=1}^{n}{}'\left\{\frac{(a_i-a_j)\beta_{ij}+b_{ij}}{x}+\cdots\right\}f_j(x) \qquad |x|\geqq R'';$$

the terms of order x^{-2}, x^{-3}, $\cdots$ in the coefficients of $f_j(x)$ in the right hand member are of course different from the corresponding terms in (94).

On account of (81) it is always possible to determine β_{ij}, $i\neq j$, so that

$$(a_i-a_j)\beta_{ij}+b_{ij}=0.$$

When the values of β_{ij} so determined are substituted in (95), that system reduces to the form

$$(96)\quad f_i(x+1)=\left(a_i+\frac{b_{ii}}{x}\right)f_i(x)+\sum_{j=1}^{n}\left(\frac{c_{ij}}{x^2}+\cdots\right)f_j(x) \quad (i=1,\cdots,n) \qquad |x|\geqq R''.$$

Now

$$a_i\left(1+\frac{1}{x}\right)^{\frac{b_{ii}}{a_i}}=a_i+\frac{b_{ii}}{x}+\cdots;$$

and hence, changing to more convenient notation and employing relations (81), we obtain the normal system

$$(97)\qquad f_i(x+1)-a_i\left(1+\frac{1}{x}\right)^{m_i}f_i(x)=\sum_{j=1}^{n}\phi_{ij}(x)f_j(x) \qquad (i=1,\cdots,n),$$

where

$$0<|a_1|<|a_2|<\cdots<|a_n|, \qquad m_i=\frac{b_{ii}}{a_i},$$

and

$$\phi_{ij}(x)=\phi''_{ij}x^{-2}+\phi'''_{ij}x^{-3}+\cdots \qquad |x|\geqq R,$$

where $R\geqq R''$. This is the normal form which we have studied in the preceding sections.

Combining the transformations (83), (85), (92) we readily obtain

$$(98)\qquad G_i(x)=\{\Gamma(x)\}^{\alpha}\sum_{k=1}^{n}\alpha_{ik}\left[f_k(x)+\sum_{l=1}^{n}\frac{\beta_{kl}}{x}f_l(x)\right] \qquad (i=1,\cdots,n).$$

It is evident therefore that if we replace $f_i(x)$, $i=1,\cdots,n$, by the particular solution $f_{ij}(x)$, $i=1,\cdots,n$, j fixed, we obtain a particular solution of (79) which we will call $G_{ij}(x)$, $i=1,\cdots,n$. Doing this for $j=1,\cdots,n$, we have n particular solutions

$$G_{1j}(x),\ G_{2j}(x),\ \cdots,\ G_{nj}(x) \qquad (j=1,\cdots,n),$$

where

$$G_{ij}(x) = \{\Gamma(x)\}^{\alpha} \sum_{k=1}^{n} \alpha_{ik} \left[f_{kj}(x) + \sum_{l=1}^{n} \frac{\beta_{kl}}{x} f_{lj}(x) \right] \qquad (i,j=1,\cdots,n). \tag{99}$$

Let us associate with (79) the corresponding equation

$$G_i(x-1) = \sum_{j=1}^{n} A_{ij}(x-1) G_j(x) \qquad (i=1,\cdots,n). \tag{100}$$

Now there is a P-region, as we have seen, in which the functions $f_{ij}(x)$ are all analytic. It follows from (99) that the functions $G_{ij}(x)$ likewise are all analytic in the same region. By means of (100) the functions of each of these solutions may be extended across the plane to the left; and in this way it may be shown that each of the n^2 functions $G_{ij}(x)$ is analytic throughout the entire plane except at the singularities of $A_{ij}(x)$ and the points congruent to them on the left.

Let us again write

$$f_{ij}(x) = a_j^x x^{m_j} U_{ij}(x) \qquad (i,j=1,\cdots,n).$$

If we substitute these values for $f_{ij}(x)$ in (99) we have

$$G_{ij}(x) = \{\Gamma(x)\}^{\alpha} a_j^x x^{m_j} V_{ij}(x), \qquad (i,j=1,\cdots,n),$$

where

$$V_{ij}(x) = \sum_{k=1} \alpha_{ik} \left[U_{kj}(x) + \sum_{l=1}^{n} \frac{\beta_{kl}}{x} U_{ij}(x) \right].$$

From (78) it follows that when x approaches infinity in the positive direction along any line parallel to the real axis we have

$$\lim V_{ij}(x) = \alpha_{ij}.$$

This result and the fact that the determinant $|\alpha_{ij}|$ is different from zero lead easily to the conclusion that the n particular solutions $G_{ij}(x)$ are independent. The method of proof is that employed for showing the independence of the solutions $f_{ij}(x)$ in the preceding section. Hence the general solution of (79) is

$$G_i(x) = \sum_{j=1}^{n} \omega_j(x) G_{ij}(x) \qquad (i=1,\cdots,n),$$

where the function $\omega_j(x)$, $j = 1, \cdots, n$, are arbitrary periodic functions of period 1.

The principal results of the section may be stated in the following theorem:

Let there be given the system of equations

$$G_i(x+1) = x^{\alpha} \sum_{j=1}^{n} a_{ij}(x) G_j(x) \qquad (i=1,\cdots,n),$$

where

1) *α is a constant;*

2) *the functions* $a_{ij}(x)$ *are single-valued and*

$$a_{ij}(x) = a_{ij} + a'_{ij}x^{-1} + a''_{ij}x^{-2} + \cdots \qquad (i, j = 1, \cdots, n) \qquad |x| > R';$$

3) *the constants* a_{ij} *are such that the roots* $\rho = a_i$ *of the equation*

$$|a_{ij} - \delta_{ij}\rho| = 0$$

are in absolute value different from each other and from zero.

Associate with the given system the corresponding one

$$G_i(x-1) = \sum_{j=1}^{n} A_{ij}(x-1)G_j(x) \qquad (i = 1, \cdots, n).$$

Then the given set of equations has the fundamental system of solutions

$$G_{1j}(x),\ G_{2j}(x),\ \cdots,\ G_{nj}(x) \qquad (j = 1, \cdots, n),$$

determined in the preceding pages and having the following properties: Each of the n^2 *functions is analytic throughout the finite plane except at the singularities of* $A_{ij}(x)$ *and the points congruent to them on the left. The general solution of the system is*

$$G_i(x) = \sum_{j=1}^{n} \omega_j(x)G_{ij}(x) \qquad (i = 1, \cdots, n),$$

where the functions $\omega_j(x), j = 1, \cdots, n$, *are arbitrary periodic functions of period* 1. *Further, if* x *approaches infinity in the positive direction along any line parallel to the real axis we have*

$$\lim G_{ij}(x)\{\Gamma(x)\}^{-\alpha} a_j^{-x} x^{-m_j} = \alpha_{ij},$$

where the constants α_{ij} *are determined by equations* (90) *and the constants* m_j *are those introduced in* (97).

Let us now consider the single difference equation of the nth order

$$\begin{aligned} &H(x+n) + (x+n)^{\alpha} b_1(x) H(x+n-1) + (x+n)^{\alpha}(x+n-1)^{\alpha} \\ &\quad \times b_2(x) H(x+n-2) + \cdots + (x+n)^{\alpha} \cdots (x+1)^{\alpha} x^{\alpha} b_n(x) H(x) = 0 \end{aligned} \tag{101}$$

where α is a constant and $b_i(x)$ is single-valued and

$$b_i(x) = b_i + b'_i x^{-1} + b''_i x^{-2} + \cdots \qquad (i = 1, \cdots, n) \qquad |x| > R,$$

and where the constants b_i are such that the roots $a_1, \cdots, a_n$ of the equation

$$\rho^n + b_1\rho^{n-1} + b_2\rho^{n-2} + \cdots + b_{n-1}\rho + b_n = 0 \tag{102}$$

are in absolute value different from each other and from zero.

Making the substitution

$$H(x) = \{\Gamma(x)\}^{\alpha} \bar{H}(x) \tag{103}$$

we have

$$\bar{H}(x+n)+b_1(x)\bar{H}(x+n-1)+\cdots+b_n(x)\bar{H}(x)=0. \tag{104}$$

It is evident that this equation is equivalent to the following system

$$\begin{aligned}&\bar{H}_1(x+1)=\sum_{j=1}^{n}\{-b_j(x)\}\bar{H}_j(x)=0,\\ &\bar{H}_i(x+1)=\bar{H}_{i-1}(x) \qquad (i=2,\cdots,n),\end{aligned} \tag{105}$$

where

$$\bar{H}_n(x)\equiv\bar{H}(x). \tag{106}$$

Now the characteristic equation [compare (80)] associated with (105) is readily reduced to the form (102).

If we solve (105) for $\bar{H}_i(x)$ in terms of $\bar{H}_i(x+1)$, $i=1,\cdots,n$, and in the result write $x-1$ for x, we have

$$\begin{aligned}&\bar{H}_i(x-1)=\bar{H}_{i+1}(x) \qquad (i=1,\cdots,n-1),\\ &\bar{H}_n(x-1)=-\frac{1}{b_n(x-1)}\bar{H}_1(x)-\sum_{j=1}^{n-1}\frac{b_j(x-1)}{b_n(x-1)}\bar{H}_{j+1}(x).\end{aligned}$$

Consequently, from the foregoing theorem, we have the following conclusions: The system (105) has a fundamental system of solutions

$$\bar{H}_{1j}(x),\ \bar{H}_{2j}(x),\ \cdots,\ \bar{H}_{nj}(x) \qquad (j=1,\cdots,n),$$

each function of which is analytic throughout the finite plane except at the singularities of the functions

$$\frac{1}{b_n(x)},\qquad \frac{b_j(x)}{b_n(x)} \qquad (j=1,\cdots,n),$$

and points congruent to them on the left; further, if x approaches infinity in the positive direction along any line parallel to the real axis, we have

$$\lim \bar{H}_{nj}(x)a_j^{-x}x^{-m_j}=\bar{\alpha}_{ij},$$

where $\bar{\alpha}_{ij}$ and m_j are constants corresponding to the α_{ij} and m_j of the above theorem. Since only the ratios of $\bar{\alpha}_{ij}$, j fixed, $i=1,\cdots,n$, are determined, we take $\bar{\alpha}_{nj}=1$, $j=1,\cdots,n$.

Combining (103) and (106) we have

$$H(x)=\{\Gamma(x)\}^a\bar{H}_n(x)$$

Hence we have a fundamental system of solutions $H_j(x)$, $j=1,\cdots,n$, of (101) in the form

$$H_j(x)=\{\Gamma(x)\}^a\bar{H}_{nj}(x) \qquad (j=1,\cdots,n).$$

Making use of this equation and the properties of $\bar{H}_{nj}(x)$ stated above and determining the position of the singularities from the equation itself by extending the solutions across the plane to the left, we obtain the results stated in the conclusion of the following theorem:

Given, the difference equation

$$H(x+n)+(x+n)^{\alpha}b_1(x)H(x+n-1)+\cdots+(x+n)^{\alpha}\cdots(x+1)^{\alpha}x^{\alpha}b_n(x)H(x)=0$$

or

$$\beta_n(x)H(x+n)+\beta_{n-1}(x)H(x+n-1)+\cdots+\beta_1(x)H(x+1)+H(x)=0,$$

where α is a constant and $b_i(x)$ is single-valued and

$$b_i(x)=b_i+b_i'x^{-1}+b_i''x^{-2}+\cdots \qquad (i=1,\cdots,n) \qquad |x|>R,$$

and where the constants b_i are such that the roots $a_1,\cdots,a_n$ of the equation

$$\rho^n+b_1\rho^{n-1}+\cdots+b_{n-1}\rho+b_n=0$$

are in absolute value different from each other and from zero.

This equation has the fundamental system of solutions

$$H_1(x),\ H_2(x),\ \cdots,\ H_n(x)$$

determined above and possessing the following properties: Each of the functions $H_1(x),\cdots,H_n(x)$ is analytic throughout the finite plane except at the singularities of the functions $\beta_i(x)$, $i=1,\cdots,n$, and the points congruent to them on the left. If x approaches infinity in the positive direction along any line parallel to the real axis, we have

$$\lim H_j(x)\{\Gamma(x)\}^{-\alpha}a_j^{-x}x^{-m_j}=1 \qquad (j=1,\cdots,n),$$

where m_j are constants.

The general solution of the eqation is

$$H(x)=\omega_1(x)H_1(x)+\cdots+\omega_n(x)H_n(x)$$

where $\omega_1(x),\cdots,\omega_n(x)$ are arbitrary periodic functions of period 1.

It may be observed that a modification of the foregoing method will lead to a different fundamental system of solutions of (79) and likewise of (101). We confine our attention to (79). A few remarks relative to the equation

$$g(x+1)-a\left(1+\frac{1}{x}\right)^m g(x)=\eta(x)$$

will sufficiently indicate the necessary changes. Employing the notation

$$\lambda(x)\equiv a\left(1+\frac{1}{x}\right)^m,$$

we have two formal solutions of the above equation as follows:

$$g(x) = -\sum_{i=0}^{\infty} \frac{\eta(x+i)}{\lambda(x)\lambda(x+1)\cdots\lambda(x+i)},$$

$$g(x) = \eta(x-1) + \sum_{i=1}^{\infty} \lambda(x-1)\lambda(x-2)\cdots\lambda(x-i)\eta(x-i-1).$$

The first of these, as we have seen, leads to a solution of (1). The second may also be employed in a similar way to obtain a solution of the same equation. The extension to a system of n equations is obvious. In this way a second fundamental system of solutions of (79) may be found.

Suppose further that transformation (83) is modified by the use of a function $\bar{\Gamma}(x)$ which satisfies the equation

$$\bar{\Gamma}(x+1) = x\bar{\Gamma}(x)$$

and is analytic to the left of the axis of imaginaries, this function replacing $\Gamma(x)$ in (83). This modification having been made, it will turn out that each function of the fundamental system just found is analytic throughout the finite plane except at the singularities of $a_{ij}(x)$ and the points congruent to them on the right; and their properties may be developed by a method similar throughout to that employed in the paper and with like results.

PRINCETON UNIVERSITY,
August, 1910.